SOPHOS

Sophos NAC 版本 3.3

配置指南

文档日期：2009 年 7 月



目录

1 NAC Manager 最佳使用方式

1.1 总体最佳使用方式

本节包含应用于展开部署 Sophos NAC，以及使用 NAC Manager 的最佳使用方式。这些最佳使用方式是 NAC Manager 中普遍的使用方式。

1.1.1 展开部署网络访问控制

进程	步骤
通过 Sophos Enterprise Console 来保护使用 Sophos NAC 的计算机。	1. 在 Sophos Enterprise Console 中运行 **保护计算机向导**。
查看 NAC Manager 报告，以决定当前的遵照状态。	1. 使用 NAC Manager 中的报告，以决定用户的遵照状态。 **注:** NAC Manager 报告就遵照策略的用户怎样使用 NAC 受管理的策略，提供了实际的说明。 2. 使用 NAC Manager 中的报告，以了解用户将要收到的消息是否适当。 **注:** 在您将策略模式更改为 “调整” 或 “强制实施” 之前，用户不会收到消息。您将在以下步骤中完成此任务。
如果需要，请更新 NAC Manager 配置文件。	1. 更新 Sophos Anti-virus 和/或 Sophos Client Firewall 配置文件。 验证这些配置文件中是否包含正确的操作系统，消息发送，以及调整措施。 2. 使用 NAC Manager 中的报告，以了解配置文件的更新是否适当。
实施调整策略。	1. 更新受到管理的策略。将**策略模式**从**仅限报告**更改为**调整**。 2. 使用 NAC Manager 中的报告，以了解当前的遵照状态。 **注:** 一段时间后，非遵照和部分遵照的终结点计算机应该被调整为遵照。

进程	步骤
如果需要，创建或更新访问模板。	1. 创建或更新访问模板。 **注:** 如果您计划使用代理强制实施来强制实施网络访问，请创建或更新代理强制实施器访问模板。如果您计划使用 DHCP 强制实施来强制实施网络访问，请创建或更新 DHCP 强制实施器访问模板。要了解更多信息，请参见 测试访问模板验证强制实施设置准确无误 （第4页）。 2. 使用 NAC Manager 中的报告，以了解访问模板是否给与终结点计算机正确的网络访问。
实施强制实施策略。	1. 更新受到管理的策略。将**策略模式**从**调整**更改为**强制实施**。 2. 使用 NAC Manager 中的报告，以了解当前的遵照状态。 **注:** 一段时间后，非遵照的终结点计算机必须调整，或者，这些用户必须被拒绝访问网络。

1.1.2 测试访问模板验证强制实施设置准确无误

最佳使用方式	描述
添加访问模板到策略中，以查看是否指派了适当的访问模板到终结点计算机上。 要了解更多有关测试策略或展开部署 Sophos NAC，请参见 展开部署网络访问控制 （第3页）。	确保针对各个访问模板，对访问状态执行了正确的强制实施措施。验证免除项目是否已被免除。查看 NAC Manager 中的代理强制实施器报告，DHCP 强制实施器报告，或 DHCP 免除项目报告，以查看在终结点计算机上应用了哪个访问模板，应用该访问模板的原因，以及强制实施措施的详情。

1.1.3 使用 Save As New 按钮

最佳使用方式	描述
使用 Save As New 按钮另存现有的配置文件，或者，访问模板为新文件，并进行更新。	如果您不想更改或无法更改现有的配置文件，或者，访问模板，那么，另存为新文件，使您能够复制这些配置文件或者，访问模板。
使用 “Save as New” 按钮，可以更新已经应用于策略中的配置文件或访问模板，除非您想要所作的更改立即生效。	如果您更新现有的，已经应用于策略中的配置文件，或者，访问模板，那么，所作的更改会立即生效，并会在下一次代理获取策略时，应用到终结点计算机上。因此，如果您想要所作的更改立即生效，请使用 “Save As New” 按钮。

1.1.4 使用锁定功能

最佳使用方式	描述
锁定策略，配置文件，访问模板，以及网络资源，可以避免无意的更改。	锁定这些 NAC Manager 项目可以避免无意的更改。管理员只能解锁他们锁定的项目。系统管理员可以解锁所有的项目。 **注:** 要保证整个策略保持受保护的状态，您必须锁定所有配置文件，访问模板，以及与策略关联的网络资源，和策略本身。

1.2 策略最佳使用方式

本节提供针对策略的最佳使用方式。将使用以下的策略约定:

- **Policy Mode（策略模式）：** 策略模式决定策略怎样评估终结点计算机；在 NAC Manager 中生成报告发送的信息；以及是否发送消息给用户，是否执行调整措施，和/或采取强制实施措施。
- **Profiles（配置文件）：** 配置文件允许您确定想要在终结点计算机上评估的项目，如：操作系统，以及应用程序。
- **Access Templates （访问模板）：** 访问模板决定怎样允许终结点计算机进行网络访问。

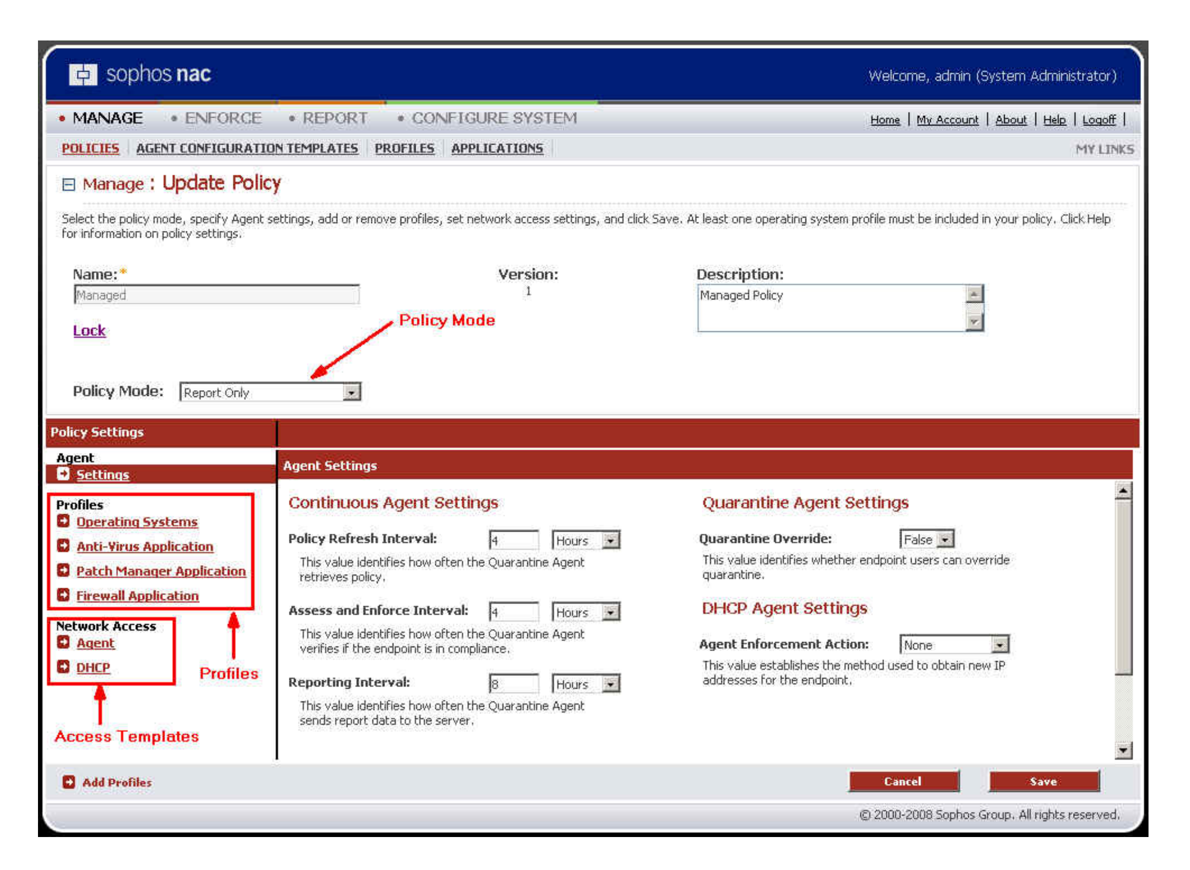


图1：策略约定示例

1.2.1 指定恰当的策略模式

重要: 您必须验证针对“仅限报告”和“调整”模式的相应的访问模板是否与策略关联。如果您应用某强制实施器访问，在“仅限报告”或“调整”模式中避免网络访问的模板，那么，所有的终结点计算机都将被拒绝访问，不管它们实际的策略遵照状态如何。要强制实施某策略遵照状态，您必须更改强制实施的策略模式。

最佳使用方式	描述
使用“仅限报告”模式评估您公司的遵照状况。	仅限报告模式，使您能够通过报告发送，搜集有关您公司中的，策略遵照状态的信息。此模式是最不干扰用户的模式。
使用调整模式，报告和调整用户，以便它们遵照已定义的策略。	调整模式提供一种方式，以报告和调整用户，以便它们遵照已定义的策略。此模式还使您能够，在开启强制实施之前，获得策略遵照的情况。
使用强制实施模式，以报告，调整，以及强制实施网络遵照。如	强制实施模式提供一种方式，以报告，调整，和强制实施网络遵照。在策略中所选的（代理和/或 DHCP）访问

最佳使用方式	描述
果用户没有遵照策略，它们会被拒绝网络访问。	模板决定网络访问。如果有多个模板应用到某个特定的访问状态中，第一个满足该状态的模板会被使用。

1.2.2 只有在网络访问绝对必要时，才使用隔离覆盖

最佳使用方式	描述
只有在网络访问绝对必要，并且安全风险极小或没有时，才设置隔离覆盖为 **true**。	设置隔离覆盖为真，可以使用户从隔离区中删除终结点计算机，即使该终结点计算机没有遵照策略。

1.2.3 维护策略只保留必要的配置文件

最佳使用方式	描述
维护策略只保留必要的配置文件。 从所有策略中删除已过时的配置文件。	维护策略只保留防病毒，个人防火墙，反间谍软件， 以及操作系统，这样能够容易地维护和支持策略。

1.2.4 在策略中添加和优先化配置文件

最佳使用方式	描述
将操作系统配置文件添加到策略中，然后优先化它们。	策略必须包括针对您想要评估的各个操作系统的，操作系统配置文件。首先优先化最重要的操作系统。 如果这些操作系统之一，没有安装到终结点计算机上，那么，具有最高优先级的操作系统配置文件将被用来决定遵照状态和措施，并且不会评估该策略中的其它配置文件。 例如，如果 Windows XP 和 Windows 2000 是要求的操作系统，并且 Windows XP 是首选的

最佳使用方式	描述
	操作系统，那么，将两种操作系统的配置文件添加到策略中，优先化 Windows XP 为首选，确保 Windows XP 配置文件中的 Else 条件设置为 Non-Compliant，并且包括针对非遵照用户的消息。在这种情形中，如果某种节点计算机没有安装任何所要求的操作系统，那么，该终结点计算机处于非遵照状态，会向用户显示消息，并且不会评估该策略中的其它配置文件。
添加相应的应用程序配置文件到策略中，然后优先化它们。	例如，如果您在策略中有多个防病毒配置文件，那么，请优先化最重要的防病毒配置文件为首选。

1.2.5 验证访问模板是否指派给了策略

最佳使用方式	描述
删除所有策略中已过时和不再使用的访问模板。	维护只包括针对已实施的强制实施类型的访问模板的策略。此最佳使用方式使得无论在策略模式下，都能容易地进行网络访问的排疑解难。
验证相关的访问模板是否指派给了策略。	依照默认值，各个策略都会自动被访问模板填充。请确保应用了正确的访问状态到各个访问状态中。 您必须优先化或删除相应的访问模板。如果有多个模板应用到某个特定的状态中，第一个满足该状态的模板会被使用。 **重要:** ■ 如果您应用某强制实施器访问，在“仅限报告”或“调整”模式中避免网络访问的模板，那么，所有的终结点计算机都将被拒绝访问，不管它们实际的策略遵照状态如何。要强制实施某策略遵照状态，您必须更改强制实施的策略模式。 ■ 如果您从某特定的访问状态中删除所有的代理强制实施器，那么，您就是对该状态允许所有的流出通讯流。

1.3 配置文件最佳使用方式

本节提供配置文件的最佳使用方式。将使用以下的配置文件约定:

- **Profiles（配置文件）：** 配置文件允许您确定您想要在终结点计算机上评估的项目，如：操作系统，以及应用程序。配置文件定义条件，遵照状态，消息，以及调整措施。配置文件可以确保策略易于配置和更新，因为对某配置文件所作的更改，可以在该配置文件所在的所有策略中生效。
- **Profile Types（配置文件类型）：** 配置文件类型可以将配置文件分类。配置文件将根据配置文件类型被放置到策略中。
- **Operating Systems（操作系统）：** 您添加到配置文件的项目所支持的操作系统。
- **Installed（已安装）：** 首先被评估的功能，以决定是否安装了应用程序。如果已安装了应用程序，会出现已配置的消息，并且将会评估剩下的应用程序功能。如果**尚未**安装应用程序，会出现已配置的消息，并且**不会**评估剩下的应用程序功能。操作系统使用 Installed 功能，然后检查服务包。
- **Message （消息）：** 表明是否向用户显示某消息的列表。
- **消息图标（Message Icon）：** 显示 Message 窗口的图标，以便您能创建消息。
- **条件（Condition）：** 在评估过程中使用的依据，以决定终结点计算机的遵照状态，以及要在终结点计算机上采取的措施。
- **遵照状态（Compliance State）：** 各个条件可以与遵照状态，部分遵照状态，或非遵照状态相关联。

  重要: 终结点计算机的遵照状态是根据策略中的配置文件来决定的。总的遵照状况，取决于最低限度的遵照状况。如果 Sophos NAC 决定某终结点计算机遵照防病毒配置文件，但是非遵照防火墙配置文件，那么，总的遵照状况为非遵照。

- **代理类型（Agent Types）：** 支持功能的代理类型。
- **Operating Systems（操作系统）：** 支持功能的操作系统。
- **Condition Parameter（条件参数）：** 测试版本的参数。

  注: 在配置文件中指定版本，可以为维护应用程序版本提供最灵活的手段。

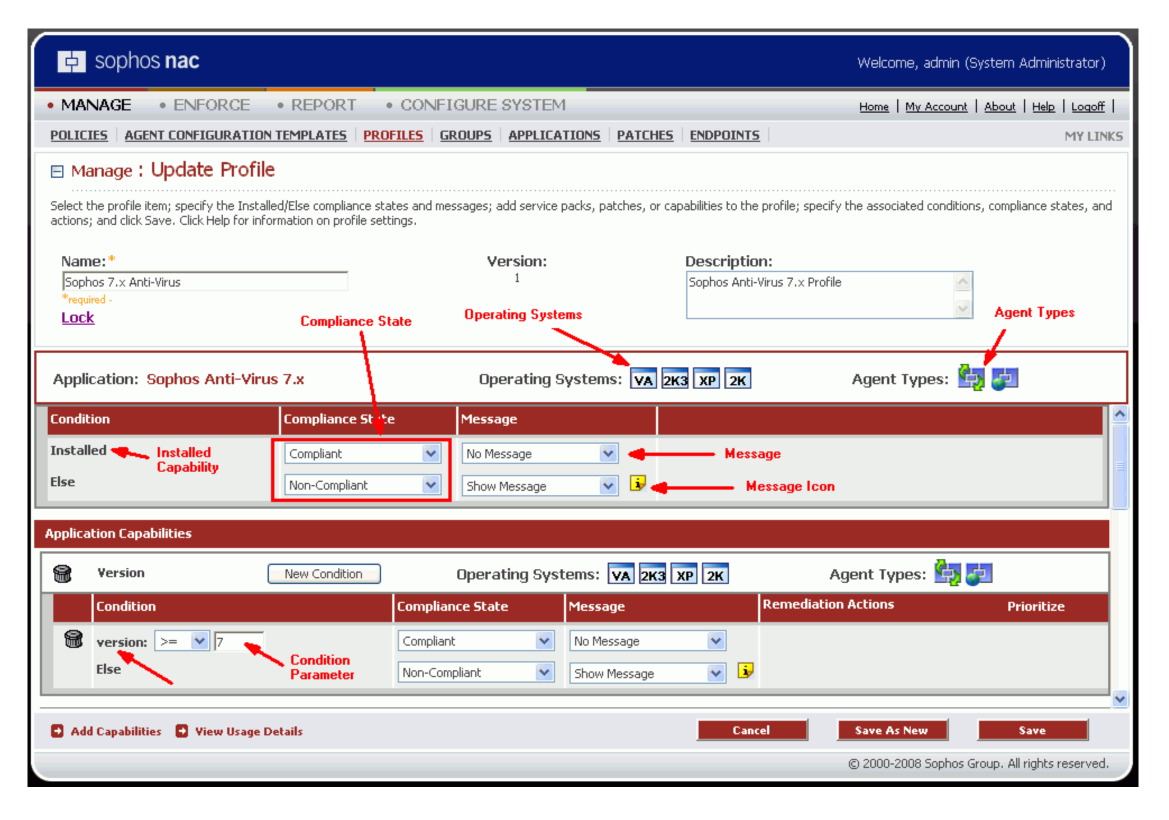


图2：配置文件约定示例

1.3.1 使用预设的配置文件创建可立即应用的配置文件

最佳使用方式	描述
使用预设的配置文件作为指南。	使用预设的配置文件： ■ 为了演示，试用，或验证等试验，您可以不用改动地使用预设的配置文件。 ■ 为了实际应用的部署，您可以复制（存储为新文件）预设的配置文件，并自定义消息发送，添加更多的条件，更改条件，等等，或者，直接使用预设的配置文件作为创建新的配置文件的指南。 对于预设的 Windows Update Profile，Sophos 建议您针对受管理的终结点计算机使用此配置文件，确保 Windows Update 工具安装到受管理的终结点计算机上，并且已启用 Automatic Updates。此配置文件会自动被添加到预设的默认和受管理的策略中。

1.3.2 添加功能到配置文件

功能是应用程序的功能集，它们可以被评估，以决定遵照状态。Sophos NAC 首先将确保某个操作系统或应用程序是使用 Installed 功能安装的。一旦软件验证了某个应用程序已安装，它将评估终结点计算机上的所有其它的功能。

注: 可用的应用程序功能，取决于应用程序软件的设计。某些功能可能无法提供给应用程序所支持的特定的操作系统，或者，无法提供给应用程序的所有版本。如果不支持某个功能，该功能不会显示。如果某个功能支持某些操作系统，不支持其它的一些操作系统，那么，该功能只会在所支持的操作系统中显示。

最佳使用方式	描述
添加测试应用程序的功能，以确保它足以保护终结点计算机。	确保应用程序已安装，并不足以确保该应用程序能够有效地保护终结点计算机。Sophos 建议您添加功能，如: Last Scan Grace Period 或 Signature Grace Period，用于测试应用程序，以确保它能够足以保护终结点计算机。
使用支持您的公司安全策略的功能。	例如，您可能会有某个策略，要求防病毒应用程序每周运行一次系统扫描，或者，您可能会有某个安全策略，认为实时扫描已可以提供足够的保护。在前一种情况中，您可能会想在配置文件中包括 Scan 功能；然而，在后一种情况中，您可能不会包括 Scan 功能。
使用 Grace Period 功能（Last Scan Grace Period 和 Signature Grace Period）与使用 Date 功能（Last Scan Date 和 Signature Date）。	Grace Period 允许您设置配置文件后，就不用再管它，这意味着最低限度的维护工作。 Grace Period 和 Date 功能不应该同时使用，除非条件经过彻底测试。可能会出现预期之外的结果。
使用所有可用的功能对大多数终结点计算机进行安全评估。	当可能对多数终结点计算机进行安全评估时，使用所有可用的功能（除了不要同时使用 Grace Period 和 Date 功能之外）。只有在它们会影响您的 NAC 部署或工作流程时，才从配置文件中删除功能。

1.3.3 指定条件和遵照状态

最佳使用方式	描述
为与预想的网络访问有关的条件指派遵照状态。	■ 使用遵照允许网络访问。 ■ 使用部分遵照，限制网络访问或隔离；或者，允许完全网络访问，但是显示消息，并且执行调整措施。 ■ 使用非遵照拒绝或限制网络访问，显示消息，以及执行调整措施。 终结点计算机的遵照状态是根据策略中的配置文件来决定的。总的遵照状况，取决于最低限度的遵照状况。如果 Sophos NAC 决定某终结点计算机遵照防病毒配置文件，但是非遵照防火墙配置文件，那么，总的遵照状况为非遵照。
添加新的条件以测试多个值，以设置不同的遵照状态，或者，以指定基于遵照状态的不同的消息/调整措施。	例如，针对 Grace Period，您可以决定某终结点计算机的签名文件可以过期5天，但是，只有当签名文件过期10天后，才会拒绝网络访问。对于这种情况，可以添加新的条件，即在5天之内，终结点计算机处于遵照状态，会向用户显示提醒消息，并且允许网络访问。添加另外一个条件，即在10天之内，终结点计算机处于部分遵照状态，会向用户显示提醒消息，并且允许网络访问。如果终结点计算机的签名文件已过期10天以上，会显示提醒消息，并且拒绝网络访问。
对于多个条件，请按照您想要评估它们的次序，优先化它们。	一旦某个条件被满足，关联的遵照状态，消息，以及调整措施就会被使用，并且没有该能力的附加的条件会被评估。 例如，通过优先化某个部分遵照（Partially Compliant）的条件优先于某个非遵照（Non-Compliant）的条件，您可以确保部分遵照的条件会优先被评估，这样，只有非遵照的终结点计算机才会被拒绝网络访问。
请确保遵照状态，消息，以及调整措施匹配所选择的条件。	所有的能力都以默认的顺序显示条件和遵照状态。如果您更改某个条件，请确保遵照状态与您预想要评估的一致。此外，如果您更改条件和遵照状态，您可能想要向用户显

最佳使用方式	描述
	示不同的消息，或者，在终结点计算机上执行不同的调整措施。 例如：默认的顺序可能是，如果防火墙是启用的，那么，终结点计算机为 遵照（Compliant）；否则，（在这种情况下防火墙没有启用），终结点计算机为非遵照（Non-Compliant）。因此，如果您更改条件为不启用（Not Enabled），那么，您应该同时更改相关的遵照状态，以决定如果防火墙没有启用，那么，终结点计算机为非遵照（Non-Compliant）；否则（即防火墙已启用），终结点计算机为遵照（Compliant）。
使用支持您的安全策略的条件和遵照状态。	例如，您可能会有某项安全策略，认定如果实时保护没有启用，那么，终结点计算机将被视为非遵照；或者，您可能会有某项安全策略，认定如果实时保护没有启用，那么，终结点计算机将被视为部分遵照。在前一种情况下，您将确保终结点计算机被被认定为非遵照状态，并且拒绝网络访问。在后一种情况下，您将调整部分遵照状态的终结点计算机，同时并不会影响网络访问。
对于 Version 功能，请确保版本号中包括正确的有效值位数。	例如：如果您创建的某个条件指定 == 8，并且终结点计算机上的版本号为 8.1，那么，当软件比较 8.1 与条件中的 8（一位有效值）时，该条件视为满足。但是，如果您创建的某个条件指定 ==8.0，并且终结点计算机上的版本号为 8.1，那么，当软件比较 8.1 与条件中的 8.0（两位有效值）时，该条件视为不满足。
对于防病毒和反间谍应用程序，请测试在 Date 能力中使用 == 操作符。	如果您在为防病毒或反间谍软件应用程序定义配置文件，并且您要使用 ==（等于）操作符来指定 Date 功能（Last Scan Date 和 Signature Date），请确保从终结点计算机中返回的日期使用的是 MM/DD/YYYY 格式。如果应用程序返回的日期是 MM/DD/YYYY HH:MM:SS 格式，那么，检测可能会失败，即使在终结点计算机上的日期与在条件中指定的值是完全一致的。要避免这个问题，请您在定义日期时使用 >=（大于或等于），或 <=（小于或等于）操作符来替代 == 操作符。您应该在部署策略之前，测试它，确保 == 操作符不会使检测失败。

1.3.4 创建消息

只有当条件得到满足时，消息才会显示。取决于策略，可以向用户显示多消息。您应该测试所有的消息，验证它们是否准确，完备，以及相关。

重要: 请考虑到这样一种情况：有的连接到网络中的终结点计算机，并不属于贵公司。如果有这样的情况，则必须有相应说明的警告消息，因为那些终结点计算机可能运行的是不同的，或不受支持的安全应用程序。预配置的 Unmanaged 策略，是专门用于未受管理的终结点计算机。更新此策略及其关联的配置文件和消息，以相应地针对未受管理的终结点计算机。

最佳使用方式	描述
创建消息，并通过使用“仅限报告”策略模式限制它们。	创建使消息发送几乎可立即应用的配置文件。您可以通过选择“仅限报告”策略模式，限制消息。当您想要显示消息以及执行调整措施，但是并不强制实施遵照时，您可以更换到“调整”策略模式。当您也想强制实施遵照时，您可以更换到“强制实施”策略模式。要了解更多信息，请参见 展开部署网络访问控制（第3页）。
使用消息告知条件出现。	例如，创建某消息，表明防病毒签名已过期，并且 Sophos NAC 将立即更新该签名。
使用英语创建所有的消息，然后，再创建对应的非英语的消息。	代理会选择最佳可能的语言显示消息。如果非英语的消息无法显示，那么，将会以英语显示消息。如果某英语的消息不存在，而非英语的该消息又无法显示，那么，就会向用户显示空的消息对话框。此外，NAC Manager 报告显示英语的消息。如果英语的消息不存在，那么，消息栏显示为空。

1.3.5 使用调整措施

可用的调整措施，取决于应用程序的软件设计。某些调整措施，可能无法提供给应用程序所支持的某些特定的操作系统，或者，无法提供给应用程序的所有版本。如果某个调整措施支持某些操作系统，不支持其它的一些操作系统，那么，在不支持的操作系统中会显示一个 x。

最佳使用方式	描述
选择调制措施，并通过使用“仅限报告”策略模式限制它们。	创建使调整措施几乎可立即应用的配置文件。您可以通过选择“仅限报告”策略模式，限制调整措施。当您想要显

最佳使用方式	描述
	示消息以及执行调整措施，但是并不强制实施遵照时，您可以更换到“调整”策略模式。当您也想强制实施遵照时，您可以更换到“强制实施”策略模式。要了解更多信息，请参见展开部署网络访问控制（第3页）。
当执行调整措施时，创建带有“部分遵照”访问状态的条件。	如果您仅创建具有“遵照”和“非遵照”遵照状态的条件，那么，终结点计算机就会被排除在可以执行调整措施的遵照状态之外。如果您创建具有“部分遵照”遵照状态的条件，那么，您可以提供调整措施，以确保终结点计算机及时更新，并且仅在它们过期时间过久时，才被视为处于非遵照状态。
针对大多数终结点计算机安全评估，尽可能使用所有提供的调整措施。	只有在调整措施有可能对您的部署工作造成问题时，才从配置文件中删除它们。
避免使用调整措施，如果它们会对终结点计算机上的重要工作造成干扰。	要避免使用调整措施，您可以为特定的用户另外创建不包括调整措施的配置文件，临时取消勾选现有配置文件中的调整措施，或更改用户策略为“仅限报告”策略模式。 总而言之，您应该评估调整措施会对用户有怎样的干扰，并评估不运行调整措施的风险，以及干扰执行重要工作的得失。

1.4 访问模板最佳使用方式

本节提供访问模板的最佳使用方式。访问模板决定怎样允许终结点计算机进行网络访问。Sophos NAC 支持代理 和 DHCP 强制实施。当访问模板被应用到 NAC Manager 中的遵照，部分遵照，或者，非遵照访问状态中时，网络访问会与策略评估一道被强制实施。要了解更多有关访问模板的信息，请参见 NAC Manager 的帮助文件。

将使用以下的访问模板约定:

- **Network Resources（网络资源）：** 网络资源是调整措施所要求的应用程序或设备，或者，那些非遵照的终结点计算机不能访问的应用程序或设备。网络资源，既可以添加到代理强制实施器的访问模板中，也可以添加到 DHCP 强制实施器的访问模板中。
- **访问强制实施器访问模板：** 代理强制实施器访问模板，识别当使用代理隔离时，终结点计算机可以，或者不可以访问的网络资源。网络资源决定终结点计算机可以访问什么应用程序或设备。代理强制实施器访问模板只应用于运行隔离代理的终结点计算机。

- **DHCP 强制实施器访问模板：** DHCP 强制实施器访问模板指定支持 DHCP 强制实施所必需的访问设置。
- **Exemptions（免除项目）：** 免除项目，是根据各种标准，在连接网络时，不需要进行遵照状态评估的终结点计算机。免除项目，包括不能运行代理的终结点计算机，如：运行非 Windows 操作系统的终结点计算机；或者，包括不要求进行遵照评估的终结点设备，如：服务器，路由器，打印机。免除项目只用于 DHCP 强制实施。

1.4.1 创建可立即应用的访问模板

最佳使用方式	描述
创建一个几乎可立即应用的访问模板。	在策略中使用 “Policy Mode” 设置，平缓地增加对用户造成的影响。您可以通过简单的设置就能够开启强制实施，同时最低限度地更改访问模板。要了解更多信息，请参见 指定恰当的策略模式（第6页）。
在更新策略之前创建所有的访问模板。	在准备好之后，您可以更新策略，以包括您已经创建了的访问模板。

1.4.2 使用预设的访问模板作为指南

最佳使用方式	描述
使用预设的访问模板作为指南。	使用预设的访问模板： ■ 为了演示，试用，或验证等试验，您可以不用改动地使用预设的访问模板。 ■ 为了软件产品部署，您可以复制（Save As New）预设的访问模板，并自定义设置。

1.4.3 优先化网络资源，访问模板，以及免除项目

使用优先化实施应用相应的网络资源

最佳使用方式	描述
优先化较特别/严格的网络资源，访问模板，以及免除项目最先，较不特别/严格的网络资源，访问模板，以及免除项目次之。	■ **Network Resources（网络资源）：** 如果有多个网络资源应用到某个终结点计算机上，第一个匹配的网络资源将决定网络访问。可执行的网络资源先于端口/协议网络资源被评估。 ■ **Access Templates （访问模板）：** 如果有多个模板应用到某个特定的访问状态中，第一个满足该状态的访问模板会被应用。较特别/严格的访问模板提供指定的 IP 地址，或较有限的 IP 地址范围，而较不特别/严格的访问模板则提供较宽泛的 IP 地址范围。 ■ **Exemptions（免除项目）：** 如果多个免除项目应用到终结点计算机上，第一个匹配的免除项目将决定网络访问。另外，如果多个访问模板应用到特定的免除项目中，第一个包含了匹配的 DHCP 服务器或 DHCP 中继的 IP 地址的那个模板将被使用。

1.4.4 指定模板遵照状态

最佳使用方式	描述
不要选择冲突的遵照状态。	例如，如果您选择 Compliant，那么，您想要创建的是允许网络访问的模板。同样，如果您选择 Non-Compliant，那么，您想要创建的是限制网络访问需要采取调整措施的服务器。

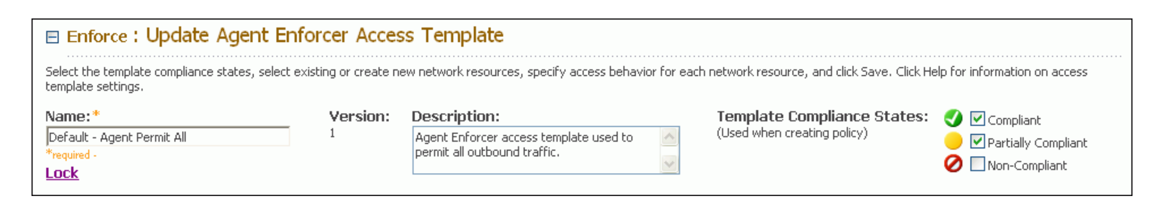


图3：模板遵照状态示例

1.4.5 为默认的访问状态指定访问模板

最佳使用方式	描述
为默认的访问状态指定访问模板。 此最佳使用方式只应用于 DHCP 强制实施。	如果使用 DHCP 强制实施，请在 NAC Manager 中的 **Configure System > Enforcer Settings** 页中，为 Default 访问状态指定相应的访问模板。 默认的访问状态是访问模板指派最根本的最后选择。因此，Sophos 建议您确保所有可能的 IP 地址都已包括在指派给 Default 访问状态的访问模板中。优先化较特别/严格的访问模板最先，并且使用 ANY - Deny All 设置识别最低优先度的访问模板。

1.4.6 创建网络资源

最佳使用方式	描述
创建精确的可执行文件网络资源。	您可以通过可执行文件或端口/协议，以及进一步通过 IP 地址和子网来识别网络资源。对可执行的网络资源，隔离代理评估来自终结点计算机的通讯流，以决定允许或拒绝哪些进程。对端口/协议和 IP 地址，隔离代理评估目的地，以决定允许或拒绝终结点访问。 网络访问可执行文件创建指南包括: ■ 可执行进程的名称必须是出现在 Windows 任务管理器中的进程标签页里的那个名称。 ■ 可执行文件的名称必须包含 .exe 扩展名，除非某进程名不包含扩展名；必须是长文件名格式；长度不能超过 64 个字符；不能使用以下字符：\ / : * ? " < > and |；不能包含文件的路径信息；不支持通配符；并且只支持 TCP 和 UDP 协议。 ■ 此软件只检测在 Winsock 级中运行的可执行进程。

2 NAC Manager 配置

2.1 NAC Manager 概述

本文档提供有关如何使用 NAC Manager 操作指导和相关信息。

限制: 不支持使用网页浏览器的按钮在 NAC Manager 中进行浏览。进行浏览和使用功能，应该使用每个页面中的菜单，链接，和按钮来实现。

2.1.1 NAC Manager 帐户名和密码

要访问 NAC Manager，您必须使用某个帐户名和密码。

在首次访问 NAC Manager 时，请使用以下帐户名和密码:

- **帐户名** = admin。
- **密码** = 您自选的密码。

在您首次访问 NAC Manager 时，会要求您更改密码。请记录下该密码，因为在您创建其它的用户帐户之前，它是您访问 NAC Manager 的唯一途径。要了解更多信息，请参见 创建帐户（第75页）。

2.1.2 查看主页

主页中提供以下控件。

- **Current Compliance:**最近七天所有被报告的终结点计算机代理的，当前遵照状态的图形化视图。要了解更多信息，请参见 运行遵照报告（第56页）。
- **Compliance Trend:**最近七天的遵照趋势的图形化视图。要了解更多信息，请参见 运行遵照报告（第56页）。
- **Server Task Status:**服务器中的各个载入器任务的状态。如果某个载入器任务失败了，请单击 **Error** 链接查看详细的出错信息。载入器任务有:
  - **Current Definition Loader:** 从 Sophos 获取防病毒软件和反间谍软件应用程序的签名的最新日期。
  - **Report Warehouse Loader:** 控制何时清空报告数据。

2.1.3 NAC Manager 图标

在 NAC Manager 中使用的图标，用于表示可能的操作，或表示含义。要了解更多有关每个图标的使用或含义的信息，请参见图标和描述表。

图标	描述
常用功能	
	增加列表中某项目的优先权。
	降低列表中某项目的优先权。
	删除某个项目。您必须确认删除列表中的项目，如：配置文件。您不必确认删除某项目中的设置，如：功能。
	必须标记某个项目或任务，它表示该项目或任务必须完成之后，才能转到其它任务，或在页面中保存信息。
	表示该项目处于解锁状态。单击该图标，锁定该项目。系统管理员和管理员可以解锁项目。
	表示该项目处于锁定状态。单击该图标，解锁该项目。系统管理员可以解锁所有的项目。管理员只能解锁他们锁定的项目。
	表示该项目已锁定，并且不能被当前的帐户用户解锁，如：被其它用户帐户锁定的自定义网络资源。
	表示页面中的某个错误必须被更正后，才能转到另一个任务或在该页面中保存信息。
	表示确认某个措施已执行，或已成功保存的消息。
	表示 NAC Manager 之外的链接。
	表示某个不能更改的预设的项目，如：某个标准的应用程序，或标准的网络资源。不过，您可以将某些标准的项目保存为新项目之后，再更改它们。
模板遵照状态	
	表示某个访问模板拟用于遵照状态中的终结点计算机。
	表示某个访问模板拟用于部分遵照状态中的终结点计算机。
	表示某个访问模板拟用于非遵照状态中的终结点计算机。
帐户	
	表示已启用的某帐户。单击该图标可以禁用该帐户。

图标	描述
	表示已禁用的某帐户。单击该图标可以启用该帐户。
配置文件和策略	
	表示某项目，如：某配置文件，应用程序，或能力，支持隔离代理。
	表示某个项目，如：某配置文件，应用程序，或功能，在 Dissolvable Agent 中受支持。
	表示某项目，如：某配置文件，应用程序，或能力，支持 Windows Vista。
	表示某项目，如：某配置文件，应用程序，或能力，支持Windows XP。
	表示某项目，如：某配置文件，应用程序，或能力，支持 Windows 2003。
	表示某项目，如：某配置文件，应用程序，或能力，支持 Windows 2000。
	表示尽管能力支持在 Windows Vista 上被支持，但是相关的调整措施不被支持。
	表示尽管能力支持在 Windows XP 上被支持，但是相关的调整措施不被支持。
	表示尽管能力支持在 Windows 2003 上被支持，但是相关的调整措施不被支持。
	表示尽管能力支持在 Windows 2000 上被支持，但是相关的调整措施不被支持。
应用程序配置文件	
	表示已针对条件定义了某消息。只有条件满足时，才会在终结点计算机上显示消息。
免除项目	
	表示 DHCP 免除项目中的 MAC 地址。
	表示 DHCP 免除项目中的软件商类型。
	表示 DHCP 免除项目中的用户类型。

图标	描述
	表示 DHCP 免除项目中的 IP 范围。
报告	
	访问与所选的代理会话报告条目关联的代理强制实施器报告。
	访问与所选的代理会话报告条目关联的 DHCP 强制实施器报告。
	评估与所选的遵照详情，代理会话，或非遵照详情报告条目关联的遵照评估的详情。

2.1.4 在 NAC Manager 中保存某项目为新项目

您可以设置项目为新项目，以便重新使用现有的设置。

建议您在更新项目的设置之前，将项目保存为新项目。可以保存为新项目的项目包括：代理配置模板，配置文件，访问模板，网络资源，以及免除。

过程

1. 单击相应的区域名称：**Manage**，**Enforce**，或 **Configure System**。
2. 单击想要重新使用的项目的区域名称。
3. 单击列表中的项目名称。
4. 单击 **Save As New**。在对话框中，为项目输入新的名称，然后单击 **OK**。

   要了解有关创建或更新项目设置的信息，请参见相应的 “创建” 主题。

2.1.5 在 NAC Manager 中查看或搜索列表项目

您可以在 NAC Manager 中，查看列表项目，或搜索特定的项目。

在 NAC Manager 的各个区域中，您可以查看创建或添加的项目列表，访问项目的详情，更新项目，或删除项目。另外，您可以使用在特定的区域中提供的搜索选项，避免出现过长的列表。

过程

1. 单击相应的区域名称：**Manage**，**Enforce**，或 **Configure System**。
2. 单击您想要查看的项目的区域名称。

   注: 为了所有**应用程序**列表页上的应用程序名称都能够正确显示，您必须在将要查看 NAC Manager 的计算机上安装亚洲语言的支持文件（通过 **Control Panel** > **Regional and Language Options** ）。

3. 如果您在 **Manage** > **Profiles 或 Applications** 中，可以使用 Search Criteria 在列表中可选地搜索特定的项目。输入或选择相应的搜索选项，并单击**Search**。

   注: 搜索列表项目的值，**不必**非要完全匹配，并且**不**区分大小写。另外，您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如，如果您在 Name 字段中，输入 M%，所有以 M 起始的名称都会显示。同样地，如果您在 Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 按照以下的说明之一做:
   - 要对列表排序，请单击相应的栏标。
   - 要查看某个项目的详情，或者更新某个项目，请单击该项目的名称。
   - 要删除某个项目，请勾选您想要删除的各个项目旁的勾选框，并单击 **Delete**。在该消息中，确认要删除的项目的列表，并单击 **OK**。

2.1.6 删除 NAC Manager 中的项目

删除 NAC Manager 中的项目，可以完全将它们从软件中删除。只有没有被其它项目使用的项目才能被删除。例如，您无法删除某个属于代理强制实施器访问模板的网络资源。您也可以使用回收站图标删除页面上的项目。

过程

1. 单击相应的区域名称：**Manage**，**Enforce**，或 **Configure System**。
2. 单击想要删除的项目的区域名称。
3. 勾选您想要删除的每个项目旁的勾选框。
4. 单击 **Delete**。
5. 在消息中，单击 **OK** 确认删除。

2.1.7 锁定或解锁 NAC Manager中的项目

锁定软件中的项目，可以防止其他的管理员更新该项目。

系统管理员可以解锁所有的项目。管理员只能解锁他们锁定的项目。

过程

1. 单击相应的区域名称：**Manage**，**Enforce**，或 **Configure System**。
2. 单击您想要锁定或解锁的项目所在的区域名。

3. 单击您想要锁定或解锁的项目旁的 **Lock** 或 **Unlock** 图标。

   图标的当前状态会显示。

   注: 有些项目，如标准的应用程序和标准的网络资源，不能够被锁定或解锁。

2.1.8 在 NAC Manager 中使用单击鼠标右键功能

单击鼠标右键功能，可以在所有列表页中使用，以及在其它某些区域中使用。

过程

1. 单击相应的区域名称： **Manage**， **Enforce**， 或 **Configure System**。
2. 单击想要管理的项目的区域名称。
3. 右击链接的名称，然后选择相应的功能。要了解更多有关区域和功能的信息，请参见 “单击鼠标右键功能 ” 表。

单击鼠标右键功能

NAC Manager 区域	描述
所有区域的标准功能	所有列示的页面包括以下标准功能：Edit，View（用于无法被编辑的标准项目），Copy，Rename，Delete，Lock/Unlock，以及 View Audit Data。 **注:** 某些功能不是列表中的所有项目都可用。
代理配置模板，配置文件，应用程序，代理强制实施器访问模板，DHCP 强制实施器访问模板，以及网络资源列表页。	指定的列表页，具有所有的标准功能之外，还有 View Usage Details 功能，它显示有关策略，配置文件，或者使用所选择的项目的访问模板的详情。
帐户列表页	帐户列表页具有所有除了 Copy 和 Lock/Unlock 的标准的功能之外，还有 Enable/Disable 功能。

2.2 管理概览

管理的范围包括管理策略所要求的所有组件。您可以从管理菜单中访问以下内容：

区域和措施	描述
应用程序	
使用标准的应用程序类型。	**应用程序类型**，将应用程序分类，并为与应用程序类型关联的所有的应用程序建立默认的策略行为。标准的应用程序类型已在软件中提供。
使用标准的应用程序。	**应用程序**是受 Sophos NAC 支持的软件应用程序。标准的应用程序已在软件中提供。应用程序会与某个应用程序类型联系起来，以决定当该应用程序的配置文件被添加到策略中时，应该怎样评估该应用程序。
代理配置模板	
创建代理配置模板。	**代理配置模板**，定义可选设置，以控制代理怎样在终结点计算机上运作。
配置文件	
为操作系统和/或应用程序创建配置文件，或者，使用预设的配置文件样本。	**配置文件**允许您确定您想要在终结点计算机上评估的项目，如：操作系统，以及应用程序。一旦创建了配置文件，它可以在策略中被组织，以及优先化。要了解更多有关配置文件组件的信息，请参见用语表（第91页）。 小技巧： ■ 使用预设的配置文件作为指南。您可以将预设的配置文件保存为新配置文件，然后，自定义消息，添加附加条件，更改遵照状态，开启调整措施等，或者，就是使用这些配置文件作为创建新的配置文件的样本。 ■ 使用预设的 Windows Update 配置文件，强制实施操作系统补丁的更新文件。要了解更多信息，请参见 *使用预设的 Windows Update 配置文件*（第33页）。
策略	
更新策略。	**策略**，根据终结点计算机上的配置文件评估，控制访问企业网络资源。策略，管理决定终结点遵照状态，消息显示，执行的调整措施，采取的强制实施措施的配置。要了解更多有关策略组件的信息，请参见用语表（第91页）。 小技巧： ■ 可以向策略中添加无限制的配置文件。 ■ 至少要有一个操作系统配置文件，必须包括在某个策略中。 ■ 策略必须包括您想要在终结点计算机上进行评估各个操作系统的，相应的操作系统配置文件。

区域和措施	描述
	■ 使用预设的策略，对受管理的和未受管理的终结点计算机，强制实施安全遵照。要了解更多信息，请参见 使用预设的策略（第26页）。

2.2.1 使用预设的策略

使用预设的策略，对受管理的和未受管理的终结点计算机，强制实施安全遵照。

在终结点计算机遵照评估的过程中，代理会获取与 Sophos Enterprise Console 中的终结点计算机的组相关联的策略。要了解更多信息，请参见 更新策略（第26页）。

- **Default:** 如果某个终结点已经安装了 Sophos Compliance Agent，并且尚未指派其它的策略，那么，此策略会被指派。依照默认值，该策略模式设置为“仅限报告”模式。如果该策略模式设置为“调整”模式，或“强制实施”模式时，它可以执行调整措施。
- **Managed:**此策略用于受 Sophos Enterprise Console 管理，并且已经安装了 Sophos Compliance Agent 的终结点计算机。依照默认值，该策略模式设置为“仅限报告”模式。如果该策略模式设置为“调整”模式，或“强制实施”模式时，它可以执行调整措施。
- **Unmanaged:**此策略用于公司外部的终结点计算机。此策略不会在终结点上执行调整措施。Dissolvable Agent 使用未受管理的策略。

注: 如果终结点计算机没有安装代理，并且没有使用 Dissolvable Agent，那么，强制实施器的设置将决定网络访问。要了解更多信息，请参见指定强制实施器设置（第76页）。

2.2.2 更新策略

策略，根据终结点计算机上的配置文件评估，控制访问企业网络资源。策略，管理决定终结点遵照状态，消息显示，执行的调整措施，采取的强制实施措施的配置。

重要: 所有的策略和策略更改都会立即在网络中生效，但是，策略不会在代理获取它之前被应用到终结点计算机上。

过程

1. 单击 **Manage** > **Policies** 。然后，单击您想要更新的策略的名称。要了解更多有关预设的策略的信息，请参见 使用预设的策略（第26页）。
2. 单击 **Policy Mode** 列表，选择策略模式。

   策略决定在遵照评估期间，使用哪个访问模板。策略模式有：Report Only，Remediate，以及 Enforce。要了解更多信息，请参见 用语表（第91页）。
3. 在左边的代理浏览区域，单击 **Settings**。
4. 如果可行，请指定继续代理设置。这些设置仅应用于运行隔离代理的终结点计算机。

   - **Policy Refresh Interval:** 确定代理获取策略的频率。该默认值是 4 小时。
   - **Assess and Enforce Interval:** 确定代理验证终结点计算机是否遵照的频率。该默认值是 4 小时。
   - **Report Interval:** 确定代理向服务器发送报告数据的频率。该默认值是 8 小时。

5. 如果可行，在 Configuration Settings 部分选择代理配置模板。

   如果没有选择配置模板，那么，代理将使用默认的设置。这些设置仅应用于运行隔离代理的终结点计算机。要了解更多信息，请参见创建代理配置模板（第30页） 和 查看代理设置（第31页）。

6. 如果可行，请指定隔离代理设置。这些设置仅应用于运行隔离代理的终结点计算机。

   - **Quarantine Override:** 确定用户是否能覆盖终结点计算机上的隔离。如果隔离覆盖设置为 True，那么，用户会被允许覆盖代理隔离。此选项使用户能够从隔离区删除终结点计算机，即使它是非遵照的。如果隔离覆盖设置为 False，那么，用户不能覆盖代理隔离，并且终结点计算机会保留在隔离区中，直到它遵照了策略。

7. 如果可行，请指定 DHCP 代理设置。这些设置仅应用于您实施了 DHCP 强制实施的情况。

   - **Agent Enforcement Action:** 建立用于为终结点计算机获取新的 IP 地址的方法。当代理启动和初始化遵照评估时，当终结点计算机遵照状态更改时，以及当在终结点计算机的策略中定义的 DHCP 强制实施器访问模板更改时，代理会获取新的 IP 地址。可用的值包括:

     - **None**终结点计算机的 IP 地址没有发布，以及没有更新。在您**不**进行 DHCP 强制实施时，选择 None。

     - **Release Renew:** 终结点计算机的 IP 地址已发布，然后通过 DHCP 服务器更新。在新的 IP 地址被获取之前，当前的 IP 地址被取消。当使用 DHCP 强制实施时，您**必须**选择 Release Renew。

8. 按照以下的说明之一做：

   - 要添加配置文件到策略中，请单击页面左下方的 **Add Profiles**，**Profile Type** 列表，选择配置文件类型，勾选您想要添加到策略中的配置文件类型旁的勾选框，然后，单击 **OK**。需要时，重复此步骤，添加附加的配置文件到策略中。

     重要: 可以向策略中添加无限制的配置文件。至少要有一个操作系统配置文件，必须包括在某个策略中。策略必须包括您想要在终结点计算机上进行评估各个操作系统的，相应的操作系统配置文件。

   - 要从策略中删除配置文件，请在左手边的 Profiles 浏览区域中单击相应的配置文件类型，然后，单击相应的配置文件旁的 **回收站**图标，将它们从策略中删除。

9. 如果您有多个操作系统配置文件，您可以为评估优先化操作系统。

   策略行为有：Required，Best，All。要了解更多信息，请参见 用语表（第91页）。

10. 如果您选择了任何应用程序配置文件，您可以指定应用程序将要在其中被评估的操作系统。同时，如果您具有多个应用程序配置文件，您可以使用箭头优先化应用程序的评估。

    注: 灰白显示的勾选框，表明不支持在某特定的操作系统上评估应用程序。

11. 在左边的 Network Access 浏览区域中，单击您想要验证或更改访问模板的强制实施类型。要为特定的访问状态添加访问模板，请单击相应的策略模式标签页，单击 **Select**，选择访问模板及其应用于的访问状态，然后，单击 **OK**。您还可以保留或删除当前的访问模板。

    您也许需要指定多个强制实施，这取决于您的网络设置。要了解更多有关强制实施类型的信息，请参见 查看策略模式和访问状态（第29页）。

    注: 依照默认值，每个策略都会自动填充基于在 NAC Manager 中预设的，各个访问状态的访问模板，以及与它们关联的模板遵照状态。请确保应用了正确的访问状态到各个访问状态中。您既可以更新预设的访问模板设置，也可以创建新的访问模板，并将它们添加到策略中，替换预设的访问模板。请注意如果您从某特定的访问状态中删除所有的代理强制实施器，那么，您就是对该状态允许所有的流出通讯流。要了解更多信息，请参见创建代理强制实施器访问模板（第46页）和 创建 *DHCP* 强制实施器访问模板（第47页）。

12. 如果需要，请使用箭头优先化 DHCP 强制实施器访问模板。

    如果有多个模板应用到某个特定的状态中，第一个满足该状态的模板会被使用。Sophos 建议您优先化较特别/严格的访问模板最先，较不特别/严格的访问模板次之。

13. 单击 **Save**。

2.2.3 查看策略模式和访问状态

以下表格将说明，根据强制实施类型，能为各策略模式提供的访问状态。

要了解更多信息，请参见 更新策略（第26页）。

策略模式	描述和访问状态
仅限报告	终结点计算机将对照指派的策略来被评估，报告信息在 NAC Manager 中生成。不会显示消息，不会执行调整措施，以及不会采取强制实施措施。 选择某个能够启用访问来自终结点计算机的通讯流的强制实施器访问模板， **重要:** 如果您应用某强制实施器访问，在“仅限报告”或“调整”模式中避免网络访问的模板，那么，所有的终结点计算机都将被拒绝访问，不管它们实际的策略遵照状态如何。要强制实施某策略遵照状态，您必须更改强制实施的策略模式。
调整	终结点计算机将对照指派的策略来被评估，报告信息在 NAC Manager 中生成。会显示消息，会执行调整措施；不过，不会采取强制实施措施。 选择某个能够启用访问来自终结点计算机的通讯流的强制实施器访问模板， **重要:** 如果您应用某强制实施器访问，在“仅限报告”或“调整”模式中避免网络访问的模板，那么，所有的终结点计算机都将被拒绝访问，不管它们实际的策略遵照状态如何。要强制实施某策略遵照状态，您必须更改强制实施的策略模式。
强制实施	终结点计算机将对照指派的策略来被评估，报告信息在 NAC Manager 中生成。通过使用针对相应的访问状态的访问模板，会显示消息，会执行调整措施，会采取强制实施措施。当终结点计算机处于指派的策略中的以下状态之一时，与该状态关联的访问模板决定网络访问。 **代理状态:** ■ **No Agent Tray:** 代理没有在终结点计算机上运行。此状态会由代理强制实施器报告，如果用户没有登录到Windows 或者，代理托盘应用程序不再运行。 ■ **User Override:** 用户覆盖了隔离在终结点计算机上的代理。 ■ **Policy Retrieval Error:** 无法从终结点计算机上获取某个策略。如果代理无法从 NAC Server获取策略； 或者，根据在 **Configure System > Enforcer Settings** 区域中配置的代

策略模式	描述和访问状态
	理策略更新级别，终结点计算机遵照状态尚未更新，那么，便会存在此状态。 强制实施器状态： ■ **Policy Retrieval Error:** 根据在 **Configure System** > **Enforcer Settings** 区域中配置的 DHCP 策略更新级别，终结点计算机遵照状态尚未更新。 遵照状态： ■ **Compliant:** 评估认为终结点计算机遵照了策略。 ■ **Partially Compliant:** 评估认为终结点计算机部分遵照了策略。 ■ **Non-Compliant:** 评估认为终结点计算机没有遵照策略。

2.2.4 创建代理配置模板

代理配置模板，使管理员能够定义可选的设置，以控制代理怎样在终结点计算机上运作。代理配置模板只应用于运行 Quarantine Agent 的终结点计算机上。

一旦创建了代理配置模板，您可以将它们添加到策略中。这样在下次进行评估时，代理可以获取已指派的策略，并同时将其设置应用到终结点计算机上。要了解更多信息，请参见 更新策略（第26页）。

过程

1. 单击 **Manage** > **Agent Configuration Templates**。然后，单击页面左下方的**创建代理配置模板**。
2. 为代理配置模板，输入名称和说明。
3. 要指定代理设置，请单击 **Select**，勾选您想要添加到代理配置模板的代理设置旁的勾选框，单击 **OK**，并在需要时指定各种值。

   代理设置决定代理在终结点计算机上运行时，代理的功能。要了解更多有关特定的代理设置，以及可用值的信息，请参见 查看代理设置（第31页）。

4. 单击 **Save**。

   注: 一旦创建了代理配置模板，您可以通过右击 **Agent Configuration Templates** 列表页上的菜单选项来使用该模板查看策略，或者，在编辑该模板时，单击 **View Usage Details** 链接，查看策略。

2.2.5 查看代理设置

以下表格描述了可用的代理设置。

要了解更多有关创建代理配置模板的信息，请参见创建代理配置模板（第30页）。

注: 图标将根据优先度在终结点计算机上显示（按照降序排列：Show Registration 图标，Show Results 图标，Show Progress 图标，Show Quarantine Override 图标，Show Quarantine 图标）。如果隐藏了优先度最高的图标，那么，会显示仅次之的优先度最高的图标，表示当前的状态。如果所有的图标都隐藏了，那么，会显示"空闲"图标。另外，任何与该图标关联的的通告措施（Notify Action 设置）都不会执行。

Agent setting	描述和可用的值	默认值
日志文件生命周期	代理日志文件将以小时计算保留到终结点计算机上，直到它们被清除和重新启动。当某个代理会话进程开始后，任何日期超过所允许的生命期的值的日志文件，都会被删除。 **注:** 日志记录活动会影响运行效率；因此，建议您仅在排疑解难时，启用日志记录，并且在排疑解难完成后，禁用日志记录。日志文件在终结点计算机中的以下文件夹中：<驱动器>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs 或者，如果是 Windows Vista，则在 <驱动器>:\ProgramData\Sophos\Sophos NAC\Logs。	24
日志记录	设置代理的日志记录级别。可用的值有: ■ **日志错误和提醒**包括错误和提醒信息。 ■ **日志记录所有的消息**包括错误，提醒，以及信息消息。 ■ **日志记录所有信息和简要追踪 (Brief Trace)**包括错误，警告，信息，以及简要追踪消息。 **注:** 日志记录活动会影响运行效率；因此，建议您仅在排疑解难时，启用日志记录，并且在排疑解难完成后，禁用日志记录。日志文件在终结点计算机中的以下文件夹中：<驱动器>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs 或者，如果是 Windows Vista，则在 <驱动器>:\ProgramData\Sophos\Sophos NAC\Logs。	日志错误和提醒
Max Attempts	针对特定的操作（如：获取策略，评估/强制实施/调整策略，以及发送报告），代理将与 communication with the NAC Server 进行通	10

Agent setting	描述和可用的值	默认值
	讯的最多次数。代理在其初始启动和持续评估的间隔期间，会重试通讯；在用户启动的遵照检查期间，代理不会重试通讯。	
Retry Delay	指定在初始化与 NAC Server的另一次通讯之前，代理需要等待的时间（以秒计）。代理在其初始启动和持续评估的间隔期间，会重试通讯；在用户启动的遵照检查期间，代理不会重试通讯。	15
Save Proxy Password	保存代理服务器的密码，供随后的代理服务器身份验证请求使用。可用的值有：**Save** 和 **Do Not Save**。	不保存
Save Proxy Username	保存代理服务器的用户名，供随后的代理服务器身份验证请求使用。可用的值有：**Save** 和 **Do Not Save**。	不保存
Show Errors In Results	显示/隐藏 Results 对话框中的出错消息。可用的值有：**Show** 和 **Hide**。 如果该值是 Show，那么，出错消息会出现在 Results 对话框中，并记录到 errors.htm 文件中，该文件位于：<驱动器>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Data 或者，如果是 Windows Vista，则在 <驱动器>:\ProgramData\Sophos\Sophos NAC\Data。如果该值是Hide，出错消息会记录在 errors.htm 文件中。	Show
Show Exit	显示/隐藏Exit 菜单选项。可用的值有：**Show** 和 **Hide**。	Hide
Show Extended Errors	显示/隐藏与 NAC Server 通讯失败相关联的 Results 对话框中，扩展的出错消息。可用的值有：**Show** 和 **Hide**。 如果该值是 Show，那么，扩展的出错消息会出现在 Results 对话框中，并记录到 errors.htm 文件中，该文件位于：<驱动器>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Data 或者，如果是 Windows Vista，则在 <驱动器>:\ProgramData\Sophos\Sophos NAC\Data。	Show
Show Logging	决定是否在 About 对话框中显示 Enable Logging 勾选框。可用的值有：**Show** 和 **Hide**。	Show

2.2.6 创建配置文件

配置文件允许您定义您想要在终结点计算机上评估的项目，如：操作系统，以及应用程序。配置文件定义条件，遵照状态，消息，以及调整措施。一旦创建了配置文件，它可以在策略中被组织，以及优先化。

您可以为特定的项目创建配置文件，然后为该项目（取决于项目类型）指定关联的服务包或应用程序功能。您还可以为同一个操作系统，或者，应用程序创建多个配置文件，如果，您想为这些项目定义不同的遵照状态，消息，或调整措施。

2.2.7 配置文件指南

配置文件指南如下:

- 可以向策略中添加无限制的配置文件。
- 至少要有一个操作系统配置文件，必须包括在某个策略中。
- 策略必须包括您想要在终结点计算机上进行评估各个操作系统的，相应的操作系统配置文件。
- 一个配置文件只能有一个操作系统或应用程序。
- 一个操作系统或应用程序可以属于多个配置文件。

2.2.8 使用预设的 Windows Update 配置文件

您可以使用预设的配置文件，强制实施更新操作系统补丁。

- **Windows Update Profile:**此配置文件可以用来确保，将 Windows Update 工具安装到受管理的终结点计算机上，并且启用 Automatic Updates。如果终结点计算机没有启用 Automatic Updates，您可以在“已启用”能力中，选择 Windows Update 调整措施，启用终结点计算机上的 Automatic Updates。此配置文件会自动被添加到默认和受管理的策略中。该配置文件旨在Quarantine Agent，以及已知用户使用。
- **针对未受管理的终结点计算机的 Windows Update 配置文件：**此配置文件可以用来确保，将 Windows Update 工具安装到未受管理的终结点计算机上，并且启用 Automatic Updates。如果某终结点计算机上没有启用 Automatic Updates，您可以提供消息，指出 Windows Automatic Updates 必须被启用，以满足遵照。此配置文件会自动被添加到未受管理的策略。该配置文件旨在 Dissolvable Agent 和来宾用户使用。

2.2.9 创建操作系统配置文件

Profiles 页能够使您创建在策略中使用的操作系统配置文件。操作系统配置文件提供了手段，组织和优先化您想要在终结点计算机上评估的操作系统以及关联的服务包。在配置文件中，您可以定义决定终结点计算机遵照状态的条件，以及要在终结点计算机上显示的消息。

过程

1. 单击 **Manage** > **Profiles**。然后，单击页面中左下方的 **Create Profile** 部分。
2. 输入配置文件的名称和说明。
3. 单击 **Select Profile Item**。
4. 从 **Profile Type** 列表中，选择 **Operating System**，然后选择您想要为其创建配置文件的操作系统，然后单击 **OK**。

   重要: 策略中必须要有操作系统配置文件。如果所需的操作系统之一没有安装到终结点计算机上，那么，来自最优先的操作系统的配置文件的 “其它 “的条件遵照状况，将被用来为该未安装的操作系统配置文件类型决定遵照状况和措施，并且不会评估该策略的任何附加的配置文件。

5. 如果可行，单击 **Compliance State** 栏目列表，为以下的操作系统条件更改遵照状态。要了解更多信息，请参见确定终结点计算机遵照状态（第45页）。
   - **Installed:** 如果该操作系统已安装，该遵照状态会被应用到终结点计算机的策略评估，以及任何配置的消息显示中。
   - **Else:** 如果尚未安装任何操作系统，那么，来自策略的最优先的操作系统配置文件中的关联遵照状态，将被应用到终结点计算机的策略评估，以及任何配置的消息显示中。
6. 如果可行，单击 **Message** 栏目列表，并选择 **Show Message** 将消息添加到某个条件中。然后，单击 **Message** 图标，以所有可用的语言（支持 8 种语言）输入消息，然后，单击 **OK**。

   只有条件满足时，才会在终结点计算机上显示消息。

   注: 代理会选择最佳可能的语言在终结点计算机上显示消息。Sophos 建议您使用英语（默认的语言）创建一条消息，这样，如果使用其它语言的消息无法显示，那么，总会有消息显示给终结点计算机用户。此外，早期版本的代理，只显示使用英语（默认的语言）的消息。要了解更多有关消息的信息，请参见 *代理配置指南*。

7. 单击 **Add Service Packs**。

   注: 只有操作系统安装到了终结点计算机上，补丁包(SP)才会被评估。

8. 选择您想要添加到配置文件中的补丁包(SP)，然后，单击 **OK**。

9. 如果可行，单击 **Compliance State** 栏目列表，为每个补丁包(SP)的条件更改遵照状态。

   - **Installed:** 如果已安装了某特定的补丁包(SP)，If a particular service pack is installed,该遵照状态会被应用到终结点计算机的策略评估，以及任何配置的消息显示中。
   - **Else:** 如果尚未安装任何补丁包(SP)，那么，来自策略的最优先（最近）的补丁包(SP)配置文件中的关联遵照状态，将被应用到终结点计算机的策略评估，以及任何配置的消息显示中。

10. 如果可行，单击 **Message** 栏目列表，并选择 **Show Message** 将消息添加到某个条件中。然后，单击 **Message** 图标，以所有可用的语言（支持 8 种语言）输入消息，然后，单击 **OK**。

    只有条件满足时，才会在终结点计算机上显示消息。

11. 单击 **Save**。

    注: 一旦创建了配置文件，您可以通过右击 **Profiles** 列表页上的菜单选项来使用该配置文件查看策略，或者，在编辑该配置文件时，单击 **View Usage Details** 链接，查看策略。

2.2.10 创建应用程序配置文件

Profiles 页能够使您创建在策略中使用的应用程序配置文件。应用程序配置文件提供了手段，组织和优先化您想要在终结点计算机上评估的应用程序以及关联的功能。在配置文件中，您可以定义决定终结点计算机遵照状态的条件，以及要在终结点计算机上显示的消息或执行的调整措施。

过程

1. 单击 **Manage > Profiles**。然后，单击页面中左下方的 **Create Profile** 部分。
2. 输入配置文件的名称和说明。
3. 单击 **Select Profile Item**。
4. 在 **Profile Type** 列表中，输入或选择相应的搜索选项，然后，单击 **Search**。
5. 选择您想要为其创建此配置文件的应用程序，然后，单击 **OK**。

   注: 为了所有的应用程序名称都能够正确显示，您必须在将要查看NAC Manager 的计算机上安装亚洲语言的支持文件（通过 **Control Panel > Regional and Language Options**）。

6. 如果可行，单击 **Compliance State** 栏目列表，为以下的应用程序条件更改遵照状态。要了解更多信息，请参见确定终结点计算机遵照状态（第45页）。

   - **Installed:** 如果应用程序已经安装，该遵照状态会被应用到终结点计算机的策略评估，以及任何配置的消息显示中。
   - **Else:** 如果应用程序没有安装，该遵照状态会被应用到终结点计算机的策略评估，以及任何配置的消息显示中。

7. 如果可行，单击 **Message** 栏目列表，并选择 **Show Message** 将消息添加到某个条件中。然后，单击 **Message** 图标，以所有可用的语言（支持 8 种语言）输入消息，然后，单击 **OK**。

   只有条件满足时，才会在终结点计算机上显示消息。

   注: 代理会选择最佳可能的语言在终结点计算机上显示消息。Sophos 建议您使用英语（默认的语言）创建一条消息，这样，如果使用其它语言的消息无法显示，那么，总会有消息显示给终结点计算机用户。此外，早期版本的代理，只显示使用英语（默认的语言）的消息。要了解更多有关消息的信息，请参见 代理配置指南。

8. 单击 **Add Capabilities**。

   能力是指某个应用程序的各种功能，这些功能可以作为遵照评估的一部分被检测。功能包括用于评估的规则，它由条件，遵照状态，信息，以及调整措施（如果可行）等构成。

   只有应用程序安装到了终结点计算机上，功能才会被评估。

9. 选择您想要添加到配置文件中的功能，然后，单击 **OK**。
   要了解更多有关功能的信息，请参见查看应用程序功能和条件（第37页）。

10. 请为各个功能做以下步骤:
    a) 单击 **Condition** 栏目列表，选择条件，或在所提供的栏目中输入条件参数。

    要了解更多有关指定给某应用程序功能的条件的信息，请参见 查看应用程序功能和条件（第37页）。

    b) 单击 **Compliance State** 栏目列表，为每个条件更改遵照状态。
    c) 单击 **Message** 栏目列表，并选择 **Show Message** 将消息添加到某个条件中。然后，单击 **Message** 图标，以所有可用的语言（支持 8 种语言）输入消息，然后，单击 **OK**。

    只有条件满足时，才会在终结点计算机上显示消息。

    d) 勾选合适的 **Remediation Action** 栏目勾选框，以应用某调整措施到某条件中。

    只有条件满足时，措施才会在终结点计算机上执行。调整措施不是对所有的应用程序或应用程序功能都可用。可用的调整措施如下:

    - **Enable:**在终结点计算机上，启用防病毒或反间谍软件应用程序的实时保护，启用防火墙应用程序的防火墙，或启用 Patch Manager 应用程序的 Automatic Updates。此措施可供 Real-Time Protection 或 Enabled application 功能使用。
    - **Update:**更新终结点计算机上的签名文件。此操作可供 Signature Date 或 Signature Grace Period 功能使用。
    - **Scan:**在终结点计算机上启动扫描。此操作可供 Scan Date 或 Scan Grace Period 功能使用。

    e) 单击 **New Condition** 添加附加条件到应用程序功能。

    可用的条件取决于您在步骤9中选择的功能；如果您没有选择具有附加条件的功能，该按钮不会显示。如果您添加附加条件，您可以使用上下箭头重新优化终结点计算机评估。

11. 单击 **Save**。

    注: 一旦创建了配置文件，您可以通过右击 **Profiles** 列表页上的菜单选项来使用该配置文件查看策略，或者，在编辑该配置文件时，单击 **View Usage Details** 链接，查看策略。

2.2.11 查看应用程序功能和条件

以下的表格将说明，根据配置文件类型，能为各应用程序功能提供的条件:

要了解更多有关创建应用程序配置文件的信息，请参见创建应用程序配置文件（第35页）。

注: 可用的应用程序功能和调整措施，取决与应用程序软件的设计。某些功能和调整措施，可能无法提供给应用程序所支持的某些特定的操作系统，或者无法提供给应用程序所支持的所有版本的某个应用程序。如果不支持某个功能，该功能不会显示。如果某个功能只在某些操作系统上才被支持，那么，只有在这些操作系统中才会显示该功能。如果某个调整措施只支持某些操作系统，那么，在不支持的操作系统中会显示一个 x。

Sophos Anti-Virus

注: Sophos Anti-Virus 支持这些功能，还支持标准的防病毒，反间谍软件，HIPS，以及 IDS 应用程序功能。可用的功能取决于软件的版本。

应用程序功能	描述和可用的条件
Adware/PUA	决定在终结点计算机上检测广告软件或可能不想安装的应用程序 (PUA)。可用的条件有: ■ **Detected/Not Detected:**指定是否检测到广告软件或可能不想安装的应用程序，关联的遵照状态，以及如果条件得到满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Detected/Not Detected 条件**没有**得到满足时的消息。
受控程序	决定是否在终结点计算机上检测受控程序。受控程序在 Sophos Enterprise Console 策略中定义。可用的条件有: ■ **Detected/Not Detected:**指定是否检测到受控程序，关联的遵照状态，以及如果条件得到满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Detected/Not Detected 条件**没有**得到满足时的消息。
受 SEC 管理	决定 Sophos Anti-Virus 是受 Sophos Enterprise Console 管理，还是独立用户(stand-alone)产品。可用的条件有: ■ **Yes/No:**指定 Sophos Anti-Virus 是否受 Sophos Enterprise Console 管理，关联的遵照条件，以及如果条件得到满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Yes/No 条件**没有**得到满足时的消息。

应用程序功能	描述和可用的条件
SEC 策略	决定 Sophos Anti-Virus 是否遵照 Sophos Enterprise Console 策略。可用的条件有: ■ **Conforms/Does Not Conform:**指定 Sophos Anti-Virus 是否遵照 Sophos Enterprise Console 策略，关联的遵照条件，以及如果条件得到满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Conforms/Does Not Conform 条件**没有**得到满足时的消息。
可疑行为	决定是否在终结点计算机上检测可疑行为。可用的条件有: ■ **Detected/Not Detected:**指定是否检测到可疑行为，关联的遵照状态，以及如果条件得到满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Detected/Not Detected 条件**没有**得到满足时的消息。
可疑文件	决定是否在终结点计算机上检测可疑文件。可用的条件有: ■ **Detected/Not Detected:**指定是否检测到可疑文件，关联的遵照状态，以及如果条件得到满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Detected/Not Detected 条件**没有**得到满足时的消息。
病毒/间谍软件	决定是否在终结点计算机上检测病毒/间谍软件。可用的条件有: ■ **Detected/Not Detected:**指定是否检测到病毒/间谍软件，关联的遵照状态，以及如果条件满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Detected/Not Detected 条件**没有**得到满足时的消息。

反间谍软件或防病毒

应用程序功能	描述和可用的条件
Last Scan Date	决定应用程序的前次扫描日期是否满足在条件中指定的日期。“前次扫描日期”功能，可以用来替代“前次扫描宽限期”功能。可用的条件有: ■ **Date:** 指定在终结点计算机的前次扫描日期，关联的遵照状态，消息，以及如果条件得到满足时的措施。操作符包括：==（等于），!=（不等于），<（小于），<=（小于等于），>（大于），>=（大于等于）。 ■ **Else:**指定关联的遵照状态，消息，以及如果 Date 条件**没有**得到满足时的措施。
Last Scan Grace Period	决定应用程序的前次扫描日期目前处于条件中指定的时间范围中。“前次扫描宽限期”功能，可以用来替代“前次扫描日期”功能。可用的条件包括: ■ **Within:** 指定在终结点计算机上，确保前次扫描日期处于当前期所需的天数，关联的遵照状态，消息，以及如果条件满足时的措施。 ■ **Else:**指定关联的遵照状态，消息，以及如果 Within 条件**没有**得到满足时的措施。
Real-Time Protection	决定应用程序对终结点计算机的保护是否处于激活状态。可用的条件有: ■ **Enabled/Disabled:**指定终结点计算机上的应用程序的实时保护是启用的还是禁用的，关联的遵照状态，消息，以及如果条件得到满足时的措施。 ■ **Else:**指定关联的遵照状态，消息，以及如果 Enabled/Disabled 条件**没有**得到满足时的措施。
Signature Date	决定应用程序的签名文件日期是否满足在条件中指定的日期。Signature Date 功能，可以用来替代 Signature Grace Period 功能。可用的条件有: ■ **Date:** 指定在终结点计算机的签名文件日期，关联的遵照状态，消息，以及如果条件得到满足时的措施。操

应用程序功能	描述和可用的条件
	作符包括：==（等于），!=（不等于），<（小于），<=（小于等于），>（大于），>=（大于等于）。 ■ **Else:**指定关联的遵照状态，消息，以及如果 Date 条件**没有**得到满足时的措施。
Signature Grace Period	决定应用程序的签名文件日期目前处于条件中指定的时间范围中。签名宽限期功能，可以用来替代签名日期功能。可用的条件包括： ■ **Within:** 指定在终结点计算机上，确保签名文件日期处于当前期所需的天数，关联的遵照状态，消息，以及如果条件满足时的措施。 ■ **Else:**指定关联的遵照状态，消息，以及如果 Within 条件**没有**得到满足时的措施。
版本	决定在终结点计算机上的应用程序的版本是否满足条件。 **注:** 在终结点上评估该版本号时，使用的是在条件中指定的值的有效位数。例如：如果您创建的某个条件指定 == 8，并且终结点计算机上的版本号为 8.1，那么，当软件比较 8.1 与条件中的 8（一位有效值）时，该条件视为满足。例如：如果您创建的某个条件指定 == 8.0，并且终结点计算机上的版本号为 8.1，那么，当软件比较 8.1 与条件中的 8.0（两位有效值）时，该条件视为**不**满足。 ■ 如果在应用程序定义为要在配置文件中指定版本，那么，配置文件中可用的条件为： 　■ **Version:** 在终结点计算机上指定应用程序的版本，关联的遵照状态，以及如果条件满足时的消息。操作符包括：==（等于），!=（不等于），<（小于），<=（小于等于），>（大于），>=（大于等于）。版本必须使用 N.n.n.n 的格式，并且局限为 4 为有效值。 　■ **Else:**指定关联的遵照状态，以及如果 Version 条件**没有**得到满足时的消息。 ■ 如果应用程序被定义为在应用程序检测规则中指定的版本号，那么，配置文件可用的条件为： 　■ **Pass/Fail:** 指定终结点计算机上的评估是否通过，如果终结点计算机应用程序版本号满足在应用程序检

应用程序功能	描述和可用的条件
	测规则中指定的版本号，并指定关联的遵照状态，以及如果条件被满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Pass/Fail 条件**没有**得到满足时的消息。

评估，HIPS 或 IDS

应用程序功能	描述和可用的条件
Running	决定是否在终结点计算机上运行可执行的服务。可用的条件有: ■ **Running/Not Running:**指定在终结点计算机上是否运行可执行的服务，关联的遵照状态，消息，以及如果条件满足时的措施。 ■ **Else:**指定关联的遵照状态，消息，以及如果 Running/Not Running 条件**没有**得到满足时的措施。
版本	决定在终结点计算机上的应用程序的版本是否满足条件。 **注:** 在终结点上评估该版本号时，使用的是在条件中指定的值的有效位数。例如：如果您创建的某个条件指定 ==8，并且终结点计算机上的版本号为 8.1，那么，当软件比较 8.1 与条件中的 8（一位有效值）时，该条件视为满足。例如：如果您创建的某个条件指定 == 8.0，并且终结点计算机上的版本号为 8.1，那么，当软件比较 8.1 与条件中的 8.0（两位有效值）时，该条件视为**不**满足。 ■ 如果在应用程序定义为要在配置文件中指定版本，那么，配置文件中可用的条件为: 　■ **Version:** 在终结点计算机上指定应用程序的版本，关联的遵照状态，以及如果条件满足时的消息。操作符包括：==（等于），!=（不等于），<（小于），<=（小于等于），>（大于），>=（大于等于）。版本必须使用 N.n.n.n 的格式，并且局限为 4 为有效值。 　■ **Else:**指定关联的遵照状态，以及如果 Version 条件**没有**得到满足时的消息。

应用程序功能	描述和可用的条件
	■ 如果应用程序被定义为在应用程序检测规则中指定的版本号，那么，配置文件可用的条件为： ■ **Pass/Fail:** 指定终结点计算机上的评估是否通过，如果终结点计算机应用程序版本号满足在应用程序检测规则中指定的版本号，并指定关联的遵照状态，以及如果条件被满足时的消息。 ■ **Else:**指定关联的遵照状态，以及如果 Pass/Fail 条件**没有**得到满足时的消息。

防火墙

应用程序功能	描述和可用的条件
Enabled	决定应用程序对终结点计算机的保护是否处于激活状态。可用的条件有： ■ **Enabled/Disabled:**指定终结点计算机上的防火墙的实时保护是启用的还是禁用的，关联的遵照状态，消息，以及如果条件得到满足时的措施。 ■ **Else:**指定关联的遵照状态，消息，以及如果 Enabled/Disabled 条件**没有**得到满足时的措施。
Running	决定是否在终结点计算机上运行可执行的服务。可用的条件有： ■ **Running/Not Running:**指定在终结点计算机上是否运行可执行的服务，关联的遵照状态，消息，以及如果条件满足时的措施。 ■ **Else:**指定关联的遵照状态，消息，以及如果 Running/Not Running 条件**没有**得到满足时的措施。
版本	决定在终结点计算机上的应用程序的版本是否满足条件。 **注:** 在终结点上评估该版本号时，使用的是在条件中指定的值的有效位数。例如：如果您创建的某个条件指定 == 8，并且终结点计算机上的版本号为 8.1，那么，当软件比较 8.1 与条件中的 8（一位有效值）时，该条件视为满足。例如：如果您创建的某个条件指定 ==

应用程序功能	描述和可用的条件
	8.0，并且终结点计算机上的版本号为 8.1，那么，当软件比较 8.1 与条件中的 8.0（两位有效值）时，该条件视为不满足。 ■ 如果在应用程序定义为要在配置文件中指定版本，那么，配置文件中可用的条件为： 　■ **Version:** 在终结点计算机上指定应用程序的版本，关联的遵照状态，以及如果条件满足时的消息。操作符包括：==（等于），!=（不等于），<（小于），<=（小于等于），>（大于），>=（大于等于）。版本必须使用 N.n.n.n 的格式，并且局限为 4 为有效值。 　■ **Else:** 指定关联的遵照状态，以及如果 Version 条件**没有**得到满足时的消息。 ■ 如果应用程序被定义为在应用程序检测规则中指定的版本号，那么，配置文件可用的条件为： 　■ **Pass/Fail:** 指定终结点计算机上的评估是否通过，如果终结点计算机应用程序版本号满足在应用程序检测规则中指定的版本号，并指定关联的遵照状态，以及如果条件被满足时的消息。 　■ **Else:** 指定关联的遵照状态，以及如果 Pass/Fail 条件**没有**得到满足时的消息。

补丁管理器

应用程序功能	描述和可用的条件
Enabled	决定应用程序对终结点计算机的保护是否处于激活状态。可用的条件有： ■ **Enabled/Disabled:** 指定是否在终结点计算机上启用或禁用 Automatic Updates for the Windows Update 工具，关联遵照状态，消息，以及如果条件满足时的措施。 ■ **Else:** 指定关联的遵照状态，消息，以及如果 Enabled/Disabled 条件**没有**得到满足时的措施。

2.2.12 确定终结点计算机遵照状态

终结点计算机是否遵照策略中的配置文件决定遵照状态。软件根据为配置文件类型指派的策略行为，来评估配置文件条件。然后，软件会将所有的 NAC 评估信息汇集到策略级别，并基于最低限度的遵照状况，指派遵照状态。一旦决定了遵照状况，通过访问指派给策略的模板，可以强制实施基于该遵照状况的网络访问。

- **Compliant:** 如果在评估过程中，条件得到满足，那么，即为遵照了策略。
- **Partially Compliant:** 如果在评估过程中，条件部分得到满足，那么，即为部分遵照了策略。
- **Non-Compliant:** 如果在评估过程中，条件没有得到满足，那么，即为没有遵照策略。

2.3 强制实施概览

强制实施的范围包括设置网络资源所需的所有组件，网络访问设置，以及免除项目。您可以从强制实施菜单中访问以下内容:

区域和措施	描述
DHCP 配置向导	
运行 DHCP 配置向导	**DHCP 配置向导**可以帮助您确定网页代理服务器，调整服务器，以及与 Sophos NAC DHCP 应用实施一道使用的 DHCP 强制实施器服务器，并自动配置您的服务器定义的默认 DHCP 强制实施器访问模板。
网络资源	
创建网络资源。	**网络资源**是要求进行终结点计算机调整的应用程序或设备，或者，应该拒绝已隔离的终结点计算机访问的应用程序或设备。网络资源可以被添加到代理强制实施器的访问模板中，也可以被添加到 DHCP 强制实施器的访问模板中。 **注:** 网络资源通过使用 Quarantine Agent 用于基于客户端的隔离强制实施，或用于 DHCP 强制实施。
代理强制实施器访问模板	
创建代理强制实施器访问模板。	**代理强制实施器访问模板**，识别当执行基于客户的隔离强制实施时，终结点计算机可以，或者不可以访问的网络资源。一旦创建完成，代理强制实施器访问模板可以被指派给策略，以进行基于终结点的代理或遵照状态的强制实施访问。 **注:** 代理强制实施器访问模板只应用于运行隔离代理的终结点计算机。

区域和措施	描述
DHCP 强制实施器访问模板	
创建 DHCP 强制实施器访问模板。	**DHCP 强制实施器访问模板**指定支持 DHCP 强制实施所必需的访问设置。一旦创建之后，DHCP 强制实施器访问模板可以用于指派策略，免除项目，以及强制实施器设置。 **注：** DHCP 强制实施器访问模板只与 Sophos NAC DHCP 应用实施一道使用。
免除项目	
创建免除项目。	**免除项目**，是根据各种标准，在连接网络时，不需要进行遵照状态评估的终结点计算机。免除项目，包括不能运行代理的终结点计算机，如：运行非 Windows 操作系统的终结点计算机；或者，包括不要求进行遵照评估的终结点设备，如：服务器，路由器，打印机。 **注：** 免除项目只用于 DHCP 强制实施。
禁用或启用免除项目。	系统管理员可以禁用或启用免除项目。禁用免除项目可以允许终结点计算机被进行遵照评估。如果免除项目已被禁用，而终结点计算机没有安装 Sophos Compliance Agent，那么，终结点计算机会被作为未知项目。启用免除项目可以避免终结点计算机被进行遵照评估。

2.3.1 创建代理强制实施器访问模板

代理强制实施器访问模板页，使您能够识别当执行基于客户的隔离强制实施时，终结点计算机可以，或者不可以访问的网络资源。代理强制实施器访问模板只应用于运行隔离代理的终结点计算机。

在代理强制实施器中指定的网络资源规范终结点计算机对网络的访问。例如，如果遵照评估表明某终结点计算机是非遵照策略的，那么，与策略非遵照状态关联的代理强制实施器访问模板就会被应用，对指定的网络资源的访问要么会被允许，要么会被拒绝。要了解更多有关网络资源的信息，请参见创建网络资源（第51页）。一旦创建了访问模板，您就可以将其指派给策略。要了解更多信息，请参见更新策略（第26页）。

过程

1. 单击 **Enforce** > **Agent Enforcer Access Templates**。然后，单击页面左下方部分的 **Create Agent Enforcer Access Template**。
2. 为代理强制实施器访问模板，输入名称和说明。
3. 勾选相应的模板遵照状态旁的勾选框，以决定代理强制实施器访问模板应该怎样被指派，或者在策略中被选择。

4. 进行以下步骤之一，指定终结点计算机访问的网络资源:
   - 单击 **Select** 将现有的网络资源添加到访问模板中，选择相应的网络资源，然后，单击 **OK**。
   - 单击 **Create** 为访问模板创建新的网络资源，在相应的栏中指定信息，然后，单击 **Save**。如果需要，请重复此步骤，为访问模板创建额外的网络资源。要了解更多信息，请参见 创建网络资源（第51页）。

5. 为每个网络资源选择访问行为。选项包括:
   - **Deny:** 为网络资源拒绝所有来自终结点计算机的网络通讯流。
   - **Permit:** 为网络资源允许所有来自终结点计算机的网络通讯流。

6. 如果需要，使用箭头优先化网络资源。

   如果有多个网络资源应用到某个终结点计算机上，第一个匹配的网络资源将决定该终结点计算机进程的网络访问。Sophos 建议您优先化较特别/严格的网络资源最先，较不特别/严格的网络资源次之。可执行的网络资源先于端口/协议网络资源被评估。

7. 单击 **Save**。

   注: 单击 **View Template Details** 链接，可以按照与代理强制实施器访问模板关联的优先程度，查看应用程序和网络资源。一旦创建了代理强制实施器访问模板，您可以通过右击 **Agent Enforcer Access Templates** 列表页上的菜单选项来使用该访问模板查看策略，或者，在编辑该访问模板时，单击 **View Usage Details** 链接，查看策略。

2.3.2 创建 DHCP 强制实施器访问模板

DHCP 强制实施器访问模板使您能够指定，支持 DHCP 强制实施所必需的访问设置。DHCP 强制实施器访问模板只与 Sophos NAC DHCP 应用实施一道使用。

如果您是首次配置 DHCP 强制实施，Sophos 建议您使用 DHCP 配置向导。要了解更多信息，请参见 *运行 DHCP 配置向导*（第49页）。如果您使用高级 DHCP 配置，您可以创建或更新现有的 DHCP 强制实施器访问模板。

在 DHCP 强制实施器中指定的网络资源规范终结点计算机对网络的访问。例如，如果遵照评估表明某终结点计算机是非遵照策略的，那么，与策略非遵照状态关联的，匹配 DHCP 服务器或 DHCP 中继 IP 地址的，DHCP 强制实施器访问模板，就会被应用，对指定的网络资源的访问要么会被允许，要么会被拒绝。要了解更多有关网络资源的信息，请参见 创建网络资源（第51页）。一旦创建了访问模板，您就可以指派策略，免除项目，或强制实施器的设置。要

了解更多的信息，请参见 更新策略（第26页），创建免除项目（第52页），或 指定强制实施器设置（第76页）。

过程

1. 单击 **Enforce** > **DHCP Enforcer Access Templates**。然后，单击页面左下方部分的 **Create DHCP Enforcer Access Template**。
2. 为 DHCP 强制实施器访问模板，输入名称和说明。
3. 勾选相应的模板遵照状态旁的勾选框，以决定 DHCP 强制实施器访问模板应该怎样被指派，或者在策略，免除项目，以及强制实施器设置中被选择。
4. 选择 **Full Access** 以允许对终结点计算机进行完全的网络访问；或者，选择 **Restricted** 以指定允许或拒绝访问指定的网络资源。
5. 如果您在步骤 4 中选择了 Restricted 访问，那么，您可以选择性地勾选 **Prevent LAN Access** 勾选框，以避免终结点计算机访问局域网 (LAN)。另外，可以选择 **Permit** 或 **Deny** 以指定您想要提供的访问类型。如果您选择 Permit，那么，您只允许访问您指定的网络资源，Sophos NAC Server，以及 Dissolvable Agent 服务器；而其它所有的网络访问都会被拒绝。如果您选择 Deny，那么，您只拒绝访问您指定的网络资源；而其它所有的网络访问都会被允许。进行以下步骤之一，指定终结点计算机访问的网络资源:
   - 单击 **Select** 将现有的网络资源添加到访问模板中，选择相应的网络资源，然后，单击 **OK**。只有带有特定的 IP 地址范围（并非 ANY）的端口/协议网络资源，才可供选择。
   - 单击 **Create** 为访问模板创建新的网络资源，在相应的栏中指定信息，然后，单击 **Save**。如果需要，请重复此步骤，为访问模板创建额外的网络资源。要了解更多信息，请参见 创建网络资源（第51页）。

   重要: 当限制访问带有 **Deny** 选项时，您必须禁用网络中的 Proxy ARP，以使 DHCP 强制实施器正确地限制对终结点计算机的访问。

   注: 如果您选择 **Permit** 选项，并且在不同于安装了 Sophos NAC 的服务器上安装了 Sophos Enterprise Console，那么，您必须为 Sophos Enterprise Console 服务器创建网络资源，并将其添加到您的 DHCP 强制实施器访问模板中。

   注: 各 DHCP 强制实施器访问模板，允许某个数量的主机路由和网络路由，此数量是由在网络资源中指定的 IP 地址/子网决定的。如果您超出了限制的数量，您可以通过从访问模板中删除网络资源，或者，从访问模板中的网络资源里删除路由，来解决这个问题。

6. 您可以单击此页左下部分的 **Advanced Options**，指定额外的 DHCP 选项。高级选项包括:

   - **User Class:** 此选项允许您要么使用 DHCP 客户端的用户类别，要么使用指定的用户类别覆盖它。您可以配置您的 DHCP 服务器指派基于用户类别的 IP 地址。如果是指定的用户类别，该用户类别会应用到，基于在指派 IP 地址之前，与模板相关联的终结点遵照状态的终结点计算机上。

     重要:

     - 如果是使用DHCP客户端的用户类别,用户类别应该是字母数字组合，区分大小写，并且必须与 DHCP 服务器上的用户类匹配。
     - 如果您指定某个用户类别，并且按照 Policy Refresh Interval，Quarantine Agent 尚未获取策略，那么，代理可能不会使用相应的用户类别，因此，在正确的策略被获取之前，可能不会得到妥当地获取 IP 地址。

   - **Lease Duration:**此选项允许您要么使用 DHCP 服务器上的租约 (lease) 设定，要么使用指派的租约设定。
   - **DNS Servers:**此选项允许您指定主 DNS 服务器和副 DNS 服务器。此选项只有在您使用 Captive Portal 时才有必要选择。您可以基于它们的终结点计算机遵照状态，将未知用户或来宾用户路由到 DNS 服务器上。
   - **DHCP Server IP Scopes:** 此选项允许您指定访问模板将使用哪个 IP 范围。选择 **ANY** 勾选框，或在所提供的栏目中，输入 IP 范围中开始和结束的 IP 地址，然后，单击 **Add**。需要时，重复这些步骤，添加附加的范围。

7. 单击 **Save**。

   注: 一旦创建了 DHCP 强制实施器访问模板，您可以通过右击 **DHCP Enforcer Access Templates** 列表页上的菜单选项来使用该访问模板查看策略，或者，在编辑该访问模板时，单击 **View Usage Details** 链接，查看策略。

2.3.3 运行 DHCP 配置向导

DHCP 配置向导可以帮助您识别与 Sophos NAC DHCP 应用实施一道使用的代理，调整，Dissolvable Agent，以及 DHCP 强制实施器服务器，并自动配置您的服务器定义的默认 DHCP 强制实施器访问模板。如果您运行该向导更新设置，您将覆盖当前的 DHCP 配置，并用您在向导中定义的服务器替换默认的 DHCP 强制实施服务器中的服务器。

要了解更多有关配置 DHCP 强制实施的信息，请参见 *Sophos NAC DHCP* 配置指南。

过程

1. 单击 **Configure System** > **DHCP Configuration Wizard** 。单击 下一步 继续。
2. 按照以下的说明之一做:
   - 如果您使用代理服务器，请单击 **Yes**，然后单击 **Next**。转到下一步。
   - 如果您不使用代理服务器，请单击 **No**，然后单击 **Next**。转到步骤4。
3. 定义代理服务器需要允许访问因特网，然后单击 **Next**。

   按照以下的说明之一做:
   - 取消勾选您不想要作为代理服务器的那些服务器旁的勾选框。
   - 单击 **Add** 添加新的服务器，输入代理服务器信息，然后单击 **OK**。需要时，重复此步骤，添加额外的服务器。一旦创建之后，这些服务器可以在 **Enforce** > **Network Resources** 页面中被管理。

   注: 所选择的代理服务器将替换目前在 DHCP - Internet Access DHCP 强制实施器访问模板中的服务器。
4. 定义调整服务器需要允许调整访问，如：域控制器，然后单击 **Next**。

   按照以下的说明之一做:
   - 取消勾选您不想要作为调整服务器的那些服务器旁的勾选框。
   - 单击 **Add** 添加新的服务器，输入调整服务器信息，然后单击 **OK**。需要时，重复此步骤，添加额外的服务器。一旦创建之后，这些服务器可以在 **Enforce** > **Network Resources** 页面中被管理。

   注: 所选择的调整服务器将替换目前在 DHCP - Remediation Access DHCP 强制实施器访问模板中的服务器。
5. 按照以下的说明之一做:
   - 如果您已经安装了 Dissolvable Agent，请单击 **Yes**，然后，单击 **Next**。转到下一步。
   - 如果您尚未安装 Dissolvable Agent，请单击 **No**，然后，单击 **Next**。转到步骤7。

   注: 如果您将 Dissolvable Agent 安装在 Sophos NAC 所在的同一个服务器上，那么，您不必创建额外的 Dissolvable Agent 服务器。
6. 定义服务器托管 Dissolvable Agent，以便 DHCP 强制实施器能够允许访问它们。要求此访问，以便未知的终结点计算机，如：来宾用户，可以变成网络已知的终结点计算机。单击 **Add** 添加新的服务器，输入 Dissolvable Agent 服务器信息，然后单击 **OK**。然后，单击 **Next**。一旦创建之后，这些服务器可以在 **Configure System** > **Server Settings** 页面中被管理。

7. 定义 DHCP 强制实施将会使用的服务器。单击 **Add** 添加新的服务器，输入 DHCP 强制实施器服务器信息，然后单击 **OK**。需要时，重复此步骤，添加额外的服务器。然后，单击 **Next**。一旦创建之后，这些服务器可以在 **Configure System** > **Server Settings** 页面中被管理。
8. 单击 **Finish**。

注: 依照默认值，新的 DHCP 强制实施器服务器会被设置为只报告未知的终结点计算机访问。要对未知的终结点计算机强制实施网络访问，您必须在 **Configure System** > **Server Settings** 页面中，对每个 DHCP 强制实施器服务器更改未知的终结点计算机模式为 **Enforce**。要了解更多信息，请参见 创建 *DHCP* 强制实施器服务器（第79页）。

注: 依照默认值，策略会被设置为只报告未知的终结点计算机访问。要对已知的受管理或未受管理的终结点计算机强制实施网络访问，您必须在 **Manage** > **Policies** 页面中，对每个策略更改策略模式为 **Enforce**。要了解更多信息，请参见 更新策略（第26页）。

2.3.4 创建网络资源

网络资源是要求进行终结点计算机调整的应用程序或设备，或者，应该拒绝已隔离的终结点计算机访问的应用程序或设备。例如：您可能想要允许防病毒软件应用程序访问，或者，访问这些应用程的所在的文件服务器，或者，您可能想要阻断网络中使用公共 IP 地址的公司电子邮件应用程序或设备。网络资源可以被添加到代理强制实施器的访问模板中，也可以被添加到 DHCP 强制实施器的访问模板中。然后，访问模板可以被指派给策略，以强制实施（通过允许或拒绝）基于终结点计算机访问状态的访问。

过程

1. 单击 **Enforce** > **Network Resources** 。然后，单击页面中左下方的 **Create Network Resource** 部分。
2. 输入网络资源的名称和说明。
3. 单击 **Network Resource Type** 列表，并选择 **Port/Protocol** 或 **Executable**。

   对于在代理强制实施器访问模板中使用的可执行的网络资源，代理将评估来自终结点计算机的通讯流，以决定允许或拒绝哪些进程。对于在代理强制实施器或 DHCP 强制实施器访问模板中使用的端口/协议网络资源，代理强制实施器或 DHCP 强制实施器，将分别地评估允许或拒绝终结点计算机访问哪些目标路径。

   注: 您必须为每个可执行的应用程序分别创建网络资源。

   注: 只有端口/协议网络资源可供 DHCP 强制实施使用。

4. 按照以下的说明之一做:

    - 如果您在步骤 3 中选择了 Port/Protocol，那么，请从 **Server Category** 列表中选择服务器种类。然后，单击 **ANY** 选项，创建应用于任何端口的网络资源，或者，单击所提供的文本框旁的选项，在该文本框中输入指定的端口；选择协议；然后单击 **Add**。如果需要，请重复此步骤以添加额外的端口和协议。
    - 如果您在步骤 3 中选择了 Executable，请在 **Name** 栏中输入应用程序的可执行进程。

    重要:

    - 可执行进程的名称**必须是**出现在 **Windows 任务管理器**中的**进程**标签页里的那个名称。
    - 可执行进程的名称**必须**包含 .exe 扩展名，除非该进程名称不包含扩展名；长度**不能**超过 64 个字符；**不能**使用以下字符：\ / : * ? " < > and |；**不能**包含文件的路径信息；**不支持**通配符；并且**只支持** TCP 和 UDP 协议。
    - 此软件只检测在 Winsock 级中运行的可执行进程。

5. 或者，要指定目标服务器，请选择 **IP Address** 或 **Host Name**；并输入 IP 地址，可选子网，以及描述，或者，在相应的文本框中输入主机名和描述，然后单击 **Add**。

    如果需要，请重复此步骤添加额外的 IP 地址和子网或主机名。

    重要: 用于 DHCP 强制实施器访问模板中的，子网掩码**不是** 255.255.255.255 的那些网络资源，将会拒绝访问运行 Windows 2000 操作系统的终结点计算机。

6. 单击 **Save**。

    注: 一旦创建了网络资源，您可以通过右击 **Network Resources** 列表页上的菜单选项来使用该网络资源查看访问模板，或者，在编辑该网络资源时，单击 **View Usage Details** 链接，查看代理访问模板。

2.3.5 创建免除项目

免除文件页使您能够使用不同的标准，确定当连接到网络时，不需要进行遵照评估的终结点计算机。免除项目，包括不能运行代理的终结点计算机，如：运行非 Windows 操作系统的终结点计算机；或者，包括不要求进行遵照评估的终结点设备，如：服务器，路由器，打印机。另外，为了在整个企业中分阶段进行阶段性强制实施，您可以为此免除任何您不想要被强制实施的终结点计算机，或者网络。

注: 免除项目只用于 DHCP 强制实施。

2.3.6 创建 DHCP 标准免除项目

Exemptions 页使您能够确定当连接到网络时，不需要进行遵照评估的终结点计算机。免除项目标准和DHCP强制实施器访问模板相互配合使用，以识别免除项目和预定的操作。一旦定义的免除标准被匹配，关联的DHCP强制实施器访问模板将决定要采取的相应的网络措施。一旦您创建了免除项目，您可以在 Exemptions 列表页中优先化它们。

过程

1. 单击 **Enforce** > **Exemptions**。然后，单击页面中左下方的 **Create Exemption** 部分。
2. 输入免除项目的名称和说明。
3. 如果您想要禁用此免除项目，请勾选 **Disable Exemption** 勾选框。

   禁用免除项目可以允许终结点计算机被进行遵照评估。如果免除项目已被禁用，而终结点计算机没有安装 Sophos Compliance Agent，那么，终结点计算机会被作为未知项目。

4. 单击 **Exemption Type** 列表，然后选择 **DHCP Criteria**。
5. 在 Exemption Criteria 下，选择 **MAC Address**，**User Class**，或 **Vendor Class** 选项按钮，以指定您想要定义的免除标准，在所提供的栏目中，输入相应的 MAC 地址（或前缀），用户类，或软件商类，然后，单击 **Add**。

   必要时，重复此步骤，添加附加的免除标准。

   注: 只要将 * 符号作为结束，您可以使用 * 符号，指定通配符的免除项目。例如：如果您指定 AA* 为 MAC 地址，所有以 AA 开始的 MAC 地址都会被免除。如果您指定的 MAC 地址，不带 * 符号，那么，您必须指定您想要免除的 MAC 地址的确切地址。

6. 在访问模板下，单击 **Select** 添加 DHCP 强制实施器访问模板到免除项目中，选择相应的模板，并单击 **OK**。

   如果您没有看到需要的 DHCP 强制实施器访问模板，您可以创建一个。要了解更多信息，请参见 *创建 DHCP 强制实施器访问模板*（第47页）。

7. 单击 **Save**。

   重要: 一旦您创建了免除项目，您可以在 **Exemptions** 列表页中优先化它们。如果有多个免除项目应用到特定的终结点计算机上，第一个与该终结点计算机关联的免除项目将被使用。Sophos 建议您优先化较特别/严格的免除项目最先，较不特别/严格的免除项目次之。

2.3.7 创建 IP 范围免除项目

Exemptions 页使您能够使用 IP 范围，确定当连接到网络时，不需要进行遵照评估的终结点计算机。IP 范围免除项目，是为网络的某部分创建的免除项目。关联的 IP 强制实施器访问模板决定 DHCP 范围和要采取的相应的网络访问措施。在整个公司执行分阶段部署强制实施时，通过IP范围进行免除会很有用；您可以免除尚不想要进行强制实施的终结点计算机或网络。一旦您创建了免除项目，您可以在 Exemptions 列表页中优先化它们。

过程

1. 单击 **Enforce** > **Exemptions** 。然后，单击页面中左下方的 **Create Exemption** 部分。
2. 输入免除项目的名称和说明。
3. 如果您想要禁用此免除项目，请勾选 **Disable Exemption** 勾选框。

   禁用免除项目可以允许终结点计算机被进行遵照评估。如果免除项目已被禁用，而终结点计算机没有安装 Sophos Compliance Agent，那么，终结点计算机会被作为未知项目。

4. 单击 **Exemption Type** 列表，然后，选择 **IP Scope**。
5. 在 Exempted IP Scopes 下，单击 **Select** 将 IP 范围添加给免除项目，选择相应的范围，然后，单击 **OK**。

   如果您没有看到需要的 IP 访问，您可以创建一个。要了解更多信息，请参见 *创建 DHCP 强制实施器访问模板*（第47页）。
6. 如果需要，使用箭头优先化范围。

   如果多个范围应用到某个特定的免除项目中，第一个被满足的范围会被使用。Sophos 建议您优先化较特别/严格的范围最先，较不特别/严格的范围次之。

7. 单击 **Save**。

   重要: 一旦您创建了免除项目，您可以在 **Exemptions** 列表页中优先化它们。如果有多个免除项目应用到特定的终结点计算机上，第一个与该终结点计算机关联的免除项目将被使用。Sophos 建议您优先化较特别/严格的免除项目最先，较不特别/严格的免除项目次之。

2.3.8 禁用或启用免除项目

免除项目在创建之后会自动启用，除非您明确禁用它们。禁用免除项目可以允许终结点计算机被进行遵照评估。如果免除项目已被禁用，而终结点计算机没有安装 Sophos Compliance Agent，那么，终结点计算机会被作为未知项目。

过程

1. 单击 **Enforce** > **Exemptions** 。
2. 单击您想要启用或禁用的免除项目旁的 **Status** 列表，然后单击 **Enabled** 或 **Disabled**。

   注: 要使用预设的免除项目，如：打印机，请更改它的状态为 Enabled。

3. 单击 **Save**。

2.4 报告概览

报告区域包含遵照以及排疑解难的报告发送所需的所有组件。您可以从报告菜单访问以下区域:

区域和措施	描述
遵照报告	
使用遵照报告查看用户遵照策略的情况。	**遵照报告**由遵照详情，以及遵照摘要报告组成。 ■ 遵照报告显示那些遵照策略的终结点计算机的详情，以及在特定的时间内，遵照策略的终结点计算机的总数。使用与遵照详情报告记录关联的评估详情，查看在某个终结点计算机上执行的遵照评估的详情。
排疑解难报告	
使用排疑解难报告，可以帮助解决与访问有关的问题，与策略遵照有关的问题，与隔离有关的问题，以及与免除项目有关的问题。	**排疑解难报告**由代理会话过程报告，非遵照详情报告，代理强制实施器报告，DHCP 强制时时器，以及 DHCP 免除项目报告组成。 ■ 代理会话过程报告，显示在特定的时间内，终结点计算机上出现的所有代理会话进程和评估。 ■ 非遵照详情报告，显示那些**没有**遵照策略的终结点计算机的详情。 ■ 代理强制实施器报告，显示在给定的时段中，使用代理强制实施进行的网络访问活动。 ■ DHCP 强制实施器报告，显示在给定的时段中，使用 DHCP 强制实施进行的网络访问活动。 ■ DHCP 免除项目报告，显示在给定的时段中的 DHCP 免除项目。

区域和措施	描述
	■ 代理会话进程报告，非遵照详情报告，代理强制实施器报告，以及 DHCP 强制实施器排疑解难报告，可以提供评估详情。使用与报告记录关联的评估详情，查看在某个终结点计算机上执行的遵照评估的详情。
保存的报告	
使用保存可以方便地重新生成报告。	**保存的报告**使您能够保存和重新使用共同的报告设置，以避免非要重新输入相同的标准。任何报告配置都可以被保存和作为保存的报告重新使用。
审核	
查看审核报告，可以查找系统事件更新。	**审核报告** 提供系统发生的事件的审核过程或历史记录。事件可以包括更新，新项目，或系统活动，如：更新到当前的策略，创建新的访问模板，或帐户登录/注销 NAC Manager。

2.4.1 打印报告

您可以打印您运行的报告，或者您访问的报告记录。

过程

1. 单击 **Report** > **Compliance** 或 **Troubleshooting** 。
2. 单击 **Report Type** 列表，并选择您想要打印的报告的名称。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Computer Name 字段中，输入 M%，所有以 M 起始的计算机名都会显示。同样地，如果您在 Computer Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 单击 **Run**。
5. 单击 **Print**。

2.4.2 运行遵照报告

使用遵照报告，查看在给定的时段中，那些终结点计算机遵照了策略。遵照报告可以用来评估策略遵照的趋势。可以提供两种类型的遵照报告：

- **Compliance Detail:** 此报告提供基于某终结点计算机的最近一次代理会话进程，在给定的时段内，遵照策略的终结点计算机的详情。您可以从Compliance Detail 报告中查看评估的详情。
- **Compliance Summary:** 此报告提供在给定的时段内，遵照策略的终结点计算机的总数。

过程

1. 单击 **Report** > **Compliance** 。
2. 单击 **Report Type** 列表，并选择**Compliance Detail** 或 **Compliance Summary**。
3. 如果情况合适，单击 **Report Criteria** 旁的加号，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Computer Name 字段中，输入 M%，所有以 M 起始的计算机名都会显示。同样地，如果您在 Computer Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 单击 **Run**。

   要了解更多有关报告结果栏目的信息，请参见“栏目及说明”表。

栏目及说明

注: Compliance Summary 报告不包括以下的所有栏目。在 Compliance Summary 报告中显示的各栏目数，代表某特定项目的实例 (instance) 数。

栏目	描述
遵照状态	在遵照状态评估时指派的终结点遵照状态。要了解更多信息，请参见确定终结点计算机遵照状态（第45页）。可用的遵照状态有：Compliant（遵照），Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。
Policy Name	代理评估的策略的名称。
Policy Version	代理评估的策略的版本。如果该策略版本是最近的版本，则会显示值 **Latest**。displays. **注:** 每次策略被更新时，版本号会递增1。
Computer Name	安装代理的终结点计算机的名称。

栏目	描述
Agent ID	代理安装或初始化会话进程所在的终结点计算机的标识符。 **注:** 该 Agent ID 是软件生成的 GUID，它唯一地识别每个代理安装。
Last Assessment Date/Time	运行在报告中的时间间隔中的最近的遵照评估的日期和时间。该评估包括在终结点计算机上评估和强制实施策略的操作。评估进行的频度，取决于在策略中设置的评估和强制实施时间间隔。三连横 (---) 表明代理会话进程超出了在搜索选项中设定的时间。 **注:** 日期和时间来自访问 NAC Manager的网页浏览器的时区。
关联的报告	评估有关与遵照详情条目关联的遵照评估的详情的图标。要了解更多信息，请参见 查看评估详情（第69页）。

2.4.3 运行代理会话进程报告

使用代理会话进程报告，查看在给定的时段中，在终结点计算机上发生的所有代理会话进程和评估。代理会话进程报告可以用于排疑解难网络访问或策略遵照的问题。此报告提供有关终结点计算机上的代理进程，在终结点计算机上执行的遵照评估，以及遵照状态的任何更改的详情。您可以查看相关的代理强制实施器记录，DHCP 强制实施器记录，或来自代理会话进程报告的评估详情。

注: 在某些情况下，因为实时数据必须从多个来源合成，数据可能会不完整。

过程

1. 单击 **Report > Troubleshooting**。
2. 单击 **Report Type** 列表，并选择 **Agent Session**。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Computer Name 字段中，输入 M%，所有以 M 起始的计算机名都会显示。同样地，如果您在 Computer Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 单击 **Run**。

   要了解更多有关报告结果栏目的信息，请参见“栏目及说明”表。

栏目及说明

栏目	描述
报告条目摘要	
Computer Name	安装代理的终结点计算机的名称。
Agent ID	代理安装或初始化会话进程所在的终结点计算机的标识符。 **注：** 该 Agent ID 是软件生成的 GUID，它唯一地识别每个代理安装。
MAC 地址	安装代理的终结点计算机的 MAC 地址。在该报告中，各个 MAC 地址会被指派给 IP 地址在其旁边的同一个 NIC。
IP Address	安装代理的终结点计算机的 IP 地址。在该报告中，各个 IP 地址会被指派给 MAC 地址在其旁边的同一个 NIC。三连横 (---) 表明 NIC 没有 IP 地址。
操作系统	安装在终结点计算机上的操作系统。
Session Start	终结点计算机上的代理启动它与 Sophos NAC 会话进程的日期和时间。 **注：** 日期和时间来自访问 NAC Manager的网页浏览器的时区。
Session End	终结点计算机上的代理结束它与 Sophos NAC 会话进程的日期和时间。三连横 (---) 表明代理会话进程没有结束。 **注：** 日期和时间来自访问 NAC Manager的网页浏览器的时区。
报告条目详情	
Assessment Start	在报告中的时间间隔的遵照评估结果的第一个实例 (instance) 的时间和日期。该评估包括在终结点计算机上评估和强制实施策略的操作。评估进行的频度，取决于在策略中设置的评估和强制实施时间间隔。 **注：** 日期和时间来自访问 NAC Manager的网页浏览器的时区。
Assessment End	在报告中的时间间隔的遵照评估结果的最后一个实例 (instance) 的时间和日期。该评估包括在终结点计算机上评估和强制实施策略的操作。三连横 (---) 表明遵照评估没有结束。 **注：** 日期和时间来自访问 NAC Manager的网页浏览器的时区。
Count	在没有任何更改的评估结果中出现的遵照评估的个数。该数字计算基于策略中设置的评估和强制实施时间间隔，代理执行了多少次遵照评估。

栏目	描述
遵照状态	在遵照状态评估时指派的终结点遵照状态。要了解更多信息，请参见确定终结点计算机遵照状态（第45页）。可用的遵照状态有：Compliant（遵照），Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。
Policy Name	代理评估的策略的名称。
Policy Version	代理评估的策略的版本。如果该策略版本是最近的版本，则会显示值 **Latest**。displays. **注:** 每次策略被更新时，版本号会递增1。
关联的报告	访问代理强制实施器记录，DHCP 强制实施器记录，或有关与此代理会话进程条目关联的遵照评估的图标。如果某关联的记录可用，图标才会显示。要了解更多的信息，请参见运行代理强制实施器报告（第61页），运行 *DHCP* 强制实施器报告（第63页），或查看评估详情（第69页）。

2.4.4 运行非遵照详情报告

使用非遵照详情报告，查看在给定的时段中，根据终结点计算机最近一次的代理会话进程，哪些终结点计算机是非遵照策略或部分遵照策略的。非遵照详情报告可以用来迅速地识别那些终结点计算机没有完全遵照策略，以及没有完全遵照的原因。您可以从非遵照详情报告中查看评估的详情。

注: 在某些情况下，因为实时数据必须从多个来源合成，数据可能会不完整。

过程

1. 单击 **Report** > **Troubleshooting**。
2. 单击 **Report Type** 列表，并选择 **Non-Compliance Detail**。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Computer Name 字段中，输入 M%，所有以 M 起始的计算机名都会显示。同样地，如果您在 Computer Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 单击 **Run**。

   要了解更多有关报告结果栏目的信息，请参见“栏目及说明”表。

栏目及说明

栏目	描述
报告条目摘要	
Username	开始会话进程的用户的用户名。
Computer Name	安装代理的终结点计算机的名称。
遵照状态	在遵照状态评估时指派的终结点遵照状态。要了解更多信息，请参见确定终结点计算机遵照状态（第45页）。可用的遵照状态有：Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。
关联的报告	评估有关与非遵照详情条目关联的遵照评估的详情的图标。要了解更多信息，请参见 查看评估详情（第69页）。
报告条目详情	
配置文件名称	代理试图在终结点计算机上检测的配置文件的名称。关联的配置文件类型显示在括号中。
功能	针对部分遵照或非遵照的终结点计算机的配置文件功能。
遵照状态	条件遵照状态，只有在终结点计算机上满足条件，才会报告此状态。可用的遵照状态有：Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。

2.4.5 运行代理强制实施器报告

使用代理强制实施器报告，查看在给定的时段中，使用代理隔离强制实施进行的网络访问活动。代理强制实施器报告可以用于排疑解难隔离一个或多个终结点计算机的问题。此报告提供终结点计算机遵照状态，关联的访问模板，以及某特定的访问模板被应用的原因的有关详情。您可以代理强制实施器报告中查看评估的详情。

注: 在某些情况下，因为实时数据必须从多个来源合成，数据可能会不完整。

过程

1. 单击 **Report > Troubleshooting** 。

2. 单击 **Report Type** 列表，然后选择 **Agent Enforcer**。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Computer Name 字段中，输入 M%，所有以 M 起始的计算机名都会显示。同样地，如果您在 Computer Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 单击 **Run**。

   要了解更多有关报告结果栏目的信息，请参见“栏目及说明”表。

栏目及说明

栏目	描述
日期/时间	代理强制实施器强制实施状态更改的日期和时间。 **注:** 日期和时间来自访问 NAC Manager的网页浏览器的时区。
Agent ID	代理安装或报告了强制实施状态更改的终结点计算机的标识符。 **注:** 该 Agent ID 是软件生成的 GUID，它唯一地识别每个代理安装。
Computer Name	安装代理的终结点计算机的名称。
遵照状态	在遵照状态评估时指派的终结点遵照状态。要了解更多信息，请参见确定终结点计算机遵照状态（第45页）。可用的遵照状态有：Compliant（遵照），Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。与策略遵照状态关联的代理强制实施器访问模板决定网络访问。
模板名称（版本）	决定代理强制实施器采取的措施的访问模板的名称和版本。该访问模板的使用有其理由。要了解更多信息，请参见创建代理强制实施器访问模板（第46页）。可用的访问模板，包括以下默认模板，以及您创建的任何访问模板: ■ **Default - Agent and Internet Access Only:**用于允许访问所有 Sophos 产品，允许使用专有 IP 地址的内部网访问因特网，以及拒绝所有其它流出通讯流的代理强制实施器访问模板。

栏目	描述
	■ **Default - Agent Permit All:** 用于允许所有流出通讯流的代理强制实施器访问模板。 ■ **None** 在 Default - Agent and Internet Access Only，和 Default - Agent Permit All 模板从策略中删除，并且没有选择任何特定的公司模板的情况下，允许所有的流出通讯流的默认的访问设置。None 访问设置可以确保代理能够访问 NAC Server。
Reason:	代理强制实施器指派某特定的访问模板的理由。可用的理由有: ■ **Assessment:** 由决定遵照状态的代理执行的评估。与策略遵照状态关联的代理强制实施器访问模板决定网络访问。访问与此代理强制实施器条目关联的遵照评估详情的链接。 ■ **No Agent Tray:** 代理没有在终结点计算机上运行。此状态会由代理强制实施器报告，如果用户没有登录到 Windows 或者，代理托盘应用程序不再运行。与 No Agent Tray 代理状态关联的策略的代理强制实施器访问模板决定网络访问。 ■ **Policy Retrieval Error:** 无法从终结点计算机上获取某个策略。如果代理无法从 NAC Server 获取策略；或者，根据在 **Configure System > Enforcer Settings** 区域中配置的代理策略更新级别，终结点计算机遵照状态尚未更新，那么，便会存在此状态。 ■ **Remediate:** 该策略处于调整模式中。与调整策略模式关联的代理强制实施器访问模板决定网络访问。 ■ **Report Only:** 该策略处于仅限报告模式。与仅限报告策略模式关联的代理强制实施器访问模板决定网络访问。 ■ **User Override:** 用户覆盖了隔离在终结点计算机上的代理。与 User Override 代理状态关联的策略的代理强制实施器访问模板决定网络访问。

2.4.6 运行 DHCP 强制实施器报告

使用 DHCP 强制实施器报告，查看在给定的时段中，使用 DHCP 强制实施进行的网络访问活动。DHCP 强制实施器报告可以用于排疑解难访问网络的问

题。此报告提供终结点计算机遵照状态，关联的访问模板，以及某特定的访问模板被应用的原因的有关详情。您可以从DHCP强制实施器报告中免除设备，以及访问评估详情。

注: 在某些情况下，因为实时数据必须从多个来源合成，数据可能会不完整。

过程

1. 单击 **Report > Troubleshooting** 。
2. 单击 **Report Type** 列表，然后选择 **DHCP Enforcer**。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Returned User Class 字段中，输入 M%，所有以 M 起始的用户类别都会显示。同样地，如果您在 Returned User Class 字段中，输入不带 % 的 M，只有以名称为 M 的用户类别会出现。

4. 单击 **Run**。

   要了解更多有关报告结果栏目的信息，请参见“栏目及说明”表。要了解有关从此报告中免除设备的信息，请参见从报告中创建免除项目（第68页）。

栏目及说明

栏目	描述
报告条目摘要	
日期/时间	尝试网络访问的日期和时间。 **注:** 日期和时间来自访问 NAC Manager的网页浏览器的时区。
MAC 地址	试图连接到网络中的设备的 MAC 地址。列示的 MAC 地址将指派给与 DHCP 客户端请求关联的 NIC。
Computer Name	试图连接到网络中的设备的名称。该计算机名来自客户端的请求。
遵照状态	在遵照状态评估时指派的终结点遵照状态。要了解更多信息，请参见确定终结点计算机遵照状态（第45页）。可用的遵照状态有：Compliant（遵照），Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。与策略遵照状态关联的 DHCP 强制实施器访问模板决定网络访问。

<table>
<tr><th>栏目</th><th>描述</th></tr>
<tr><td>模板名称（版本）</td><td>决定 DHCP 强制实施器采取的措施的访问模板的名称和版本。该访问模板的使用有其理由。要了解更多信息，请参见 创建 DHCP 强制实施器访问模板（第47页）。可用的访问模板，包括以下默认模板，以及您创建的任何访问模板：

■ DHCP - Full Access: 允许完全的网络访问。

■ DHCP - Internet Access: 允许除了局域网 (LAN) 之外的所有的网络访问。

■ DHCP - Remediation Access: 拒绝除了 Sophos NAC Server 和 Dissolvable Agent 服务器之外的所有的网络访问。</td></tr>
<tr><td>Reason:</td><td>DHCP 强制实施器指派某特定的访问模板的理由。可用的理由有：

■ Assessment:由决定遵照状态的代理执行的评估。与策略遵照状态关联的 DHCP 强制实施器访问模板决定网络访问。访问与此 DHCP 强制实施器条目关联的遵照评估详情的链接。

■ Default Template:终结点计算机可能具有关联的策略或被指派为免除项目，但是找不到某关联的访问模板。在 Configure System > Enforcer Settings 区域中指定的 Default 访问模板决定网络访问。

■ Enforcer Override: 强制实施没有被检查。如果在 Configure System > Enforcer Settings 区域中勾选了 Override DHCP Enforcer 勾选框，那么，在该区域中指派的 Maintenance Mode/Enforcer Override 访问模板也决定网络访问。

■ Exempted: 终结点计算机的免除是基于在 Enforce > Exemptions 区域中定义的免除项目标准。与免除项目标准关联的访问模板决定网络访问。以下的免除理由会显示在括号中：

  ■ User Class: 被指定为免除项目的用户类别。

  ■ Vendor Class: 被指定为免除项目的软件商类别。

  ■ MAC: 被指定为免除项目的 MAC 地址。

  ■ IP Scope: 被指定为免除项目的 IP 范围。</td></tr>
</table>

栏目	描述
	■ **Maintenance Mode:** 该软件处于维护模式。在 **Configure System** > **Enforcer Settings** 区域中指定的 Mode/Enforcer Override 访问模板，会被用来决定网络访问。 ■ **Policy Retrieval Error:**根据在 **Configure System** > **Enforcer Settings** 区域中配置的 DHCP 策略更新级别，终结点计算机遵照状态尚未更新。与 Policy Retrieval Error 状态关联的 DHCP 强制实施器访问模板决定网络访问。 ■ **Remediate:**该策略处于调整模式中。与调整策略模式关联的 DHCP 强制实施器访问模板决定网络访问。 ■ **Report Only:**该策略处于仅限报告模式。与仅限报告策略模式关联的 DHCP 强制实施器访问模板决定网络访问。 ■ **Reserved:** 设备的 MAC 地址要求网络访问保留为 DHCP 服务器上的特殊设备。 ■ **System Error:** 强制实施器遇到错误，因此无法顺利完成它的操作。设置在 NAC Server上的 SystemErrors 注册键默认设置为拒绝网络访问。 ■ **Template Error:** 没有找到关联的访问模板，在 **Configure System** > **Enforcer Settings** 区域中指定的 Default 访问模板没有被使用。如果收到此错误，那么，DHCP 服务器将决定网络访问，它将不会返回用户类，并且将拒绝访问该用户。 ■ **Unknown Endpoint:** 没有遵照记录存在。在 **Configure System** > **Enforcer Settings** 区域中指定的 Unknown Endpoint 访问模板决定网络访问。
Returned User Class	通过执行强制实施的 DHCP 强制实施器返回给 DHCP 服务器的 DHCP 用户类别。
DHCP 服务器	DHCP 服务器的 IP 地址，要求来自 DHCP 强制实施器的网络访问。它是 DHCP 强制实施器软件安装所在的 DHCP 服务器。
报告条目详情	
Agent Enforcement Action	终结点计算机采取的有关指派 IP 地址的措施。初始发布和更新基于在策略中指定的代理强制实施措施的 IP 地址的终结点计算机。当代理启动和初始化遵照评估时，当终结点计算机遵照状态更改时，当策略模

栏目	描述
	式更改时，以及当在终结点计算机的策略中定义的 DHCP 强制实施器访问模板更改时，代理会获取新的 IP 地址。可用的值包括: ■ **None**终结点计算机的 IP 地址没有发布，以及没有更新。 ■ **Release Renew:** 终结点计算机的 IP 地址已发布，然后通过 DHCP 服务器更新。在新的 IP 地址被获取之前，当前的 IP 地址被取消。 ■ **Triple Dash (---):** 代理没有报告某措施。
Vendor Class	DHCP 客户端的软件商类。
DHCP Relay	DHCP 中继 IP 地址（如果出现在原始的 DHCP 要求中），被 DHCP 强制实施器用来选择 DHCP 强制实施器访问模板。如果没有使用 DHCP 中继，0.0.0.0 会显示。
Transaction ID	从 DHCP 服务器返回的活动 ID。该活动 ID 将 DHCP 客户端消息与服务器回应关联起来。

2.4.7 运行 DHCP 免除项目报告

使用 DHCP 免除报告，查看在给定的时段中的 DHCP 免除项目。DHCP 免除项目报告可以用于排疑解难访问指定为免除项目的网络的问题。

注: 在某些情况下，因为实时数据必须从多个来源合成，数据可能会不完整。

过程

1. 单击 **Report** > **Troubleshooting** 。
2. 单击 **Report Type** 列表，然后选择 **DHCP Exemption** 。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Returned User Class 字段中，输入 M%，所有以 M 起始的用户类别都会显示。同样地，如果您在 Returned User Class 字段中，输入不带 % 的 M，只有以名称为 M 的用户类别会出现。

4. 单击 **Run**。

   要了解更多有关报告结果栏目的信息，请参见“栏目及说明”表。

栏目及说明

栏目	描述
报告条目摘要	
日期/时间	尝试网络访问的日期和时间。 **注:** 日期和时间来自访问 NAC Manager的网页浏览器的时区。
模板名称（版本）	决定 DHCP 强制实施器采取的措施的访问模板的名称。要了解更多信息，请参见 *创建 DHCP 强制实施器访问模板*（第47页）。
免除项目条件名称	免除项目的名称和免除项目标准的详情。
MAC 地址	试图连接到网络中的设备的 MAC 地址。列示的 MAC 地址将指派给与 DHCP 客户端请求关联的 NIC。
Returned User Class	通过执行强制实施的 DHCP 强制实施器返回给 DHCP 服务器的 DHCP 用户类别。
DHCP 服务器	DHCP 服务器的 IP 地址，要求来自 DHCP 强制实施器的网络访问。它是 DHCP 强制实施器软件安装所在的 DHCP 服务器。
报告条目详情	
Source User Class	DHCP 用户类，如果有，将从 DHCP 客户端发送到 DHCP 服务器。
Vendor Class	DHCP 客户端的软件商类。
DHCP Relay	DHCP 中继 IP 地址（如果出现在原始的 DHCP 要求中），被 DHCP 强制实施器用来选择 DHCP 强制实施器访问模板。如果没有使用 DHCP 中继，0.0.0.0 会显示。

2.4.8 从报告中创建免除项目

您可以从DHCP强制实施器报告中，为在DHCP强制实施期间被报告的设备，创建免除项目。

基于“Exempted”原因，免除项目会显示在DHCP强制实施器报告中。如果您从报告中免除设备，那么，在设备重新连接到网络之前，它们不会作为“Exempted”出现在报告中。要了解更多有关DHCP强制实施器报告字段和描述的信息，请参见 *运行 DHCP 强制实施器报告*（第63页）。

过程

1. 单击 **Report > Troubleshooting** 。
2. 单击 **Report Type** 列表，然后选择 **DHCP Enforcer**。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Returned User Class 字段中，输入 M%，所有以 M 起始的用户类别都会显示。同样地，如果您在 Returned User Class 字段中，输入不带 % 的 M，只有以名称为 M 的用户类别会出现。

4. 单击 **Run**。
5. 勾选您想要免除的设备旁的勾选框，然后，单击 **Exempt**。
6. 确认您想要免除的设备列表，选择您想要应用到免除项目中的访问模板，然后，单击 **OK**。

   要管理或应用额外的访问模板到您创建的免除项目中，请转到 **Enforce > Exemptions** 区域。要了解更多信息，请参见 创建 *DHCP* 标准免除项目（第 53页）。

2.4.9 查看评估详情

使用评估详情，查看有关终结点计算机上执行的遵照评估的详情。

您可以从以下报告中查看评估详情：遵照详情，代理会话进程，非遵照详情，代理强制实施器，或 DHCP 强制实施器。显示的评估详情，有您查看的报告条目相关联。评估详情显示在终结点计算机上测试过的配置文件条件，测试条件的结果，基于该评估所指派的遵照状态，以及任何在该终结点计算机上采取的措施。

过程

1. 单击 **Report > Compliance or Troubleshooting** 。
2. 单击 **Report Type** 列表，并选择**Compliance Detail**，**Agent Session**，**Non-Compliance Detail**，**Agent Enforcer**，或 **DHCP Enforcer**。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Computer Name 字段中，输入 M%，所有以 M 起始的计算机名都会显示。同样地，如果您在 Computer Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 单击 **Run**。
5. 在仅限代理会话进程报告中，单击报告摘要旁的**加号**，查看相关的报告条目的详情。
6. 根据报告，单击 **Assessment Details** 图标或 **Assessment** 链接。

   要了解更多有关报告结果栏目的信息，请参见“栏目及说明”表。

栏目及说明

栏目	描述
配置文件类型评估详情	
配置文件类型	代理试图在终结点计算机上检测的配置文件类型。
遵照状态	配置文件类型遵照状态。遵照状态是配置文件的集合体，这些配置文件在终结点计算机上与要求的，最佳的，或所有的策略行为一道被评估。要了解更多信息，请参见以下的选择理由。可用的遵照状态有：Compliant（遵照），Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。
配置文件评估详情	
配置文件名称	代理试图在终结点计算机上检测的配置文件的名称。
已选择	说明是否配置文件被用于决定配置文件类型的遵照状态。如果该值为 True，那么，该配置文件被使用。如果该值为 False，那么，该配置文件没有被使用；其它的配置文件取而代之被用于决定遵照状态。要了解更多有关配置文件怎样在终结点计算机上被评估的信息，请参见以下的选择理由。
选择理由	说明为什么配置文件被用于或不被用于决定配置类型的遵照状态。这基于决定配置文件怎样对照终结点计算机上其它相同类型的配置文件被评估的策略行为。可用的值有： ■ **要求的（最佳）：** 显示是否在该终结点计算机上找到了要求的操作系统配置文件。操作系统的配置文件是必需的，并且将作为首选的配置文件进行评估。 ■ **Best:** 显示是否在该终结点计算机上找到了最佳的配置文件。策略中的某一特定类型的每个配置文件，都是在终结点计算机上被评估，最佳匹配的配置文件将被确定，并且只有与最佳匹配的文件有关的必要的措施会被执行。最佳行为使用终结点计算机上，**最大限度**遵照的配置文

栏目	描述
	件来决定策略中的该配置文件类型的遵照状况。应用程序配置文件，除非另有指定，都是以此方式被评估的。 ■ **Best (No Match):** 如果最佳评估的配置文件没有在终结点计算机上找到，则会显示。如果被评估的配置文件，没有任何一个安装到了终结点计算机上，那么，来自最优先的配置文件的“其它”的条件遵照状况，将被用来决定策略中的该配置文件类型的遵照状况和措施。如果所需的操作系统之一没有安装到终结点计算机上，那么，来自最优先的操作系统的配置文件的“其它“的条件遵照状况，将被用来为该未安装的操作系统配置文件类型决定遵照状况和措施，并且不会评估该策略的任何附加的配置文件。 ■ **All:** 如果在终结点计算机上评估所有的配置文件，则会显示。策略中某一类型的所有配置文件，都将在终结点计算机上进行评估，并且与所有配置文件相关的必要措施都会执行。所有行为使用终结点计算机上，**最低限度**遵照的配置文件来决定策略中的该配置文件类型的遵照状况。您想要在终结点计算机上避免的应用程序配置文件，也可以此方式被评估。
Detected	如果在终结点计算机上检测到了配置文件项目（操作系统或应用程序），则会显示。如果值为 True，那么，检测到了配置文件项目。如果值为 False，那么，没有检测到配置文件项目。
遵照状态	配置文件遵照状态。该遵照状态由在终结点计算机上评估的配置文件条件构成。所有的配置文件条件都会被评估，以决定该配置文件的遵照状态。可用的遵照状态有：Compliant（遵照），Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。
配置文件能力评估详情	
Profile Condition	显示对照在终结点计算机上检测到的结果的在配置文件中配置的条件。检测到的结果可能是版本，号码，或日期，或任何其它在终结点计算机上定义条件的项目。三连横 (---) 表明该条件没有定义项。
Result	条件评估的结果。如果结果为 True，那么，在配置文件定义的条件在终结点计算机得到了满足。如果结果为 False，那么，在配置文件定义的条件在终结点计算机没有得到满足。

栏目	描述
遵照状态	条件遵照状态，只有在终结点计算机上满足条件，才会报告此状态。可用的遵照状态有：Compliant（遵照），Partially Compliant（部分遵照），和 Non-Compliant（非遵照）。三连横 (---) 表明代理没有报告遵照状态。
Action Type	在终结点计算机上执行的调整措施的类型。只有当与措施相关联的条件被满足时，措施才会在终结点计算机上显示或执行。可用的措施类型有： ■ **Message:**在终结点计算机上显示消息。此措施可用于所有的能力。 ■ **Enable:**在终结点计算机上，启用防病毒或反间谍应用程序的实时保护，启用防火墙应用程序的防火墙，或启用 Patch Manager 应用程序的 Automatic Updates。此措施可供 Real-Time Protection 或 Enabled application 功能使用。 ■ **Update:**更新终结点计算机上的签名文件。此操作可供 Signature Date 或 Signature Grace Period 应用程序功能使用。 ■ **Scan:**在终结点计算机上启动引擎扫描。此操作可供 Signature Date 或 Signature Grace Period 应用程序功能使用。
Action Value	在终结点计算机上向用户显示的消息。只有联合的条件被满足时，消息才会在终结点计算机上显示。没有其它措施类型显示措施值。

2.4.10 保存报告

您可以通过更改某现有的报告的搜索和排序标准来满足您的要求，并保存报告。当报告保存后，该标准也被保存。

过程

1. 单击 **Report** > **Compliance** 或 **Troubleshooting** 。
2. 单击 **Report Type** 列表，并选择您想要保存的报告的名称。

3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Computer Name 字段中，输入 M%，所有以 M 起始的计算机名都会显示。同样地，如果您在 Computer Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 单击 **Run**。
5. 单击 **Save**。
6. 在该对话框中，在 **Report Name** 栏中输入报告名称。
7. 单击 **Save**。

2.4.11 运行保存的报告

保存的报告使您能够保存和重新使用共同的报告设置，以避免非要重新输入相同的标准。您还可以为保存的报告更新报告设置，并且不用非要保存新的报告。

过程

1. 单击 **Report** > **Saved** 。
2. 单击 **Saved Report** 列表，然后选择您想要运行的保存报告的名称。
3. 如果情况合适，单击 **Report Criteria** 旁的**加号**，然后，输入或选择相应的搜索选项。您也可以单击 **Custom Sort** 链接，扩展您的筛选选项；当报告运行时，自定义的筛选选项会暂时更改。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Computer Name 字段中，输入 M%，所有以 M 起始的计算机名都会显示。同样地，如果您在 Computer Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

4. 单击 **Run**。

2.4.12 删除保存的报告

删除保存的报告会完全将它们从软件中删除。

过程

1. 单击 **Report** > **Saved** 。
2. 单击 **Saved Report** 列表，然后选择您想要删除的保存报告的名称。
3. 单击 **Delete**。

4. 在消息中，单击 **OK** 确认删除。

2.4.13 查看审核

Audits 区域提供系统发生的事件的审核过程或历史记录。事件可以包括更新，新项目，或系统活动，如：更新到当前的策略，创建新的访问模板，或帐户登录/注销 NAC Manager.

过程

1. 单击 **Report** > **Audits** 。
2. 在所提供的区域里输入或选择适当的搜索选项，然后单击 **Search**。

   注: 您在多数字段中进行搜索时，可以使用 * 或 % 符号作为通配符。例如：如果您在 Item Name 字段中，输入 M%，所有以 M 起始的项目名都会显示。同样地，如果您在 Item Name 字段中，输入不带 % 的 M，只有以名称为 M 的项目会出现。

3. 按照以下的说明之一做：
   - 要对列表排序，请单击相应的栏标。
   - 要查看有关事件的详情，请单击 **Details** 链接。

2.5 配置系统概览

配置系统区域包括所有配置 NAC Manager 系统组件的组件。您可以从配置系统菜单中访问以下区域：

区域和措施	描述
帐户	
创建系统帐户	**帐户**允许对 NAC Manager 进行不同级别的访问。系统管理员可以为系统帐户创建名称，并定义安全角色。帐户名和密码被用来登录 NAC Manager。安全角色决定每个帐户的权限级别。
禁用或启用帐户。	系统管理员可以禁用或启用帐户。禁用某帐户可以阻止该帐户的用户登录 NAC Manager，查看系统信息，或执行任何管理功能。启用某帐户可以允许该帐户用户登录 NAC Manager，并执行由该帐户的安全角色指派的所有管理功能。
强制实施器设置	
为强制实施器指定设置。	**强制实施器设置** 指定代理强制实施器的强制实施详情，以及 DHCP 强制实施器的强制实施类型。代理强制实施器，用于基于客户的隔离强

区域和措施	描述
	制实施。DHCP 强制实施器，将与 Sophos NAC DHCP 应用实施，一道使用。
服务器设置	
创建 DHCP 强制实施器服务器。	使用此区域定义 DHCP 强制实施器服务器与 Sophos NAC DHCP 应用实施，一道使用。
创建 Dissolvable Agent 服务器。	使用此区域定义托管 Dissolvable Agent，以便 DHCP 强制实施器能够允许访问它们。
更新 NAC 代理服务器设置。	在安装NAC的过程中，您可以配置NAC使用代理服务器访问因特网。要求能够访问因特网，以便为安全应用程序下载最新的检测信息。使用此区域更新代理服务器设置，以及选择更新NAC Server IP 地址。
下载帐户详情	
更新下载帐户详情。	NAC 使用下载帐户用户名和密码，为安全应用程序下载最新的检测信息。

2.5.1 创建帐户

帐户区域，使系统管理员能够创建名称，并为系统帐户定义安全角色。帐户名和密码被用来登录 NAC Manager。安全角色决定每个帐户的权限级别。

过程

1. 单击 **Configure System** > **Accounts** 。然后，单击页面中左下方的 **Create Account** 部分。
2. 键入帐户名称。
3. 或者，可以勾选 **Disable Account** 勾选框，创建一个禁用的帐户。
4. 输入并确认帐户的密码。

   注: 如果您正在更新某个现有的帐户的密码，那么，您必须同时要输入您的帐户密码。该栏确保只有具备有效帐户的系统管理员才能更新帐户密码。

5. 选择以下安全角色之一:

   - **System Administrator:** 对 NAC Manager 中的所有区域都具有完全的访问权限。系统管理员可以创建，更新，和删除帐户。
   - **Administrator:** 对 NAC Manager 中的 Manage，Enforce，以及 Report 区域具有完全的访问权限。对 NAC Manager 中的 Configure System 区域具有读权限。管理员安全角色没有查看或管理帐户的权限。
   - **Help Desk:**对 NAC Manager 中的 Manage，Enforce，以及 Report 区域具有完全的访问权限。对 NAC Manager 中的 Manage，Enforce，以及 Configure System 区域具有读权限。桌面支持安全角色没有查看或管理帐户的权限。
   - **Guest:** 对 NAC Manager 中的所有区域具有读权限。来宾安全角色没有查看或管理帐户的权限。

   注: 所有的安全角色都可以使用导航功能，包括它们自己的帐户密码，帮助，以及有关 NAC Manager 的信息。

6. 单击 **Save**。

2.5.2 禁用或启用帐户

帐户在创建之后会自动启用，除非您明确禁用它们。禁用某帐户可以阻止该帐户的用户登录 NAC Manager，查看系统信息，或执行任何管理功能。

过程

1. 单击 **Configure System** > **Accounts** 。
2. 单击您想要禁用或启用的帐户名称旁的 **Enabled Account** 或 **Disabled Account** 图标。图标的当前状态会显示。

2.5.3 指定强制实施器设置

Enforcer Settings 页面，使您能够配置设置，指定DHCP 强制实施器或代理强制实施器怎样执行强制实施。DHCP 强制实施器与 Sophos NAC DHCP 应用实施一道使用。代理强制实施器，用于基于客户的隔离强制实施。

过程

1. 单击 **Configure System** > **Enforcer Settings** 。

2. 如果您使用代理强制实施器，请指定以下级别设置。如果您还使用DHCP强制实施器，请转到下一步；否则，请转到步骤7:

   - **Agent Policy Update Threshold:** 确定在终结点计算机被放置到隔离区之前，Quarantine Agent 必须获取策略的时间限制（以分钟，小时，或天为单位）。如果此级别被超过，终结点计算机会被放置到隔离区中，并且要求获取新的策略。同时，与策略的 Policy Retrieval Error 访问状态关联的代理强制实施器访问模板，将决定网络访问。此级别用于代理强制实施。该默认值是 8 小时。

     重要: 策略更新级别的时间设置必须总是**多于**指定给各策略的策略刷新间隔时间；否则，每次达到策略更新级别时，将由策略中的 Policy Retrieval Error 访问状态决定网络访问，终结点计算机将被放置到隔离区中。

3. 为DHCP 强制实施器指定以下的级别设置:

   - **DHCP Policy Update Threshold:** 确定从代理获取策略到策略过期之间的时间（以分钟，小时，或天为单位）。如果它过期了，则要求获取新的策略。同时，与策略的 Policy Retrieval Error 访问状态关联的 DHCP 强制实施器访问模板，将决定网络访问。此级别，用于 DHCP 强制实施，是服务器值，它可以覆盖任何由代理报告的值，但是不会影响隔离强制实施。如果设置为 0，则此级别被禁用。该默认值是 5 小时。

     注: 建议设置此级别至少**多于**指定给各策略的策略刷新间隔时间10分钟。

   - **Dissolvable Agent Compliance Threshold:** 确定未受管理的终结点计算机的遵照记录被 DHCP 强制实施器认可为有效的时间间隔（以分钟，小时，或天为单位）。如果该级别被超过，未受管理的终结点计算机会被认为是未知，直到在该终结点计算机上执行了遵照评估。同时，在步骤5中指定的 Unknown Endpoint 访问模板将决定网络访问。如果设置为0，则该级别被禁用。该默认值是 12 小时。

4. 选择相应的 DHCP 强制实施器服务器设置:

   - **Report Exemptions:** 决定DHCP 强制实施器是否报告免除项目的勾选框。如果勾选该勾选框，终结点计算机会被免除，被报告，并显示在 DHCP 免除项目报告中。如果没有勾选该勾选框，终结点计算机会被免除，但是不会被报告。要了解更多的信息，请参见*运行DHCP免除项目报告*（第67页）。
   - **Exempt DHCP Reservations:** 决定是否免除在 DHCP 服务器上配置的保留的终结点计算机的勾选框。如果勾选该勾选框，保留的终结点计算机会被从强制实施中免除。
   - **Override DHCP Enforcer:** 决定DHCP 强制实施器是否根据定义的安全策略执行强制实施的勾选框。如果勾选该勾选框，强制实施会被禁用，在步骤5中指定的 Maintenance Mode/Enforcer Override 访问模板会决定网络访问；不过，只有该终结点计算机不是定义的免除项目时，才会使用这些访问模板。

5. 要为特定的访问状态添加或更改访问模板，请单击 **Select** under DHCP Enforcer Access Templates，勾选访问模板旁的勾选框，以及模板所应用到其中的访问状态旁的勾选框，然后，单击 **OK**。您还可以保留或删除默认的访问模板。可用的访问状态如下:

   - **Unknown Endpoint:** 当非遵照的记录存在时，决定网络访问。未知的终结点计算机不会被 Sophos Enterprise Console管理，不会被免除，既没有运行 Dissolvable Agent，也没有超过在步骤2中定义的 Dissolvable Agent Compliance Threshold。当 DHCP 服务器处于 Report Only 或 Enforce 未知终结点计算机模式时，您可以选择针对未知的终结点计算机使用的访问模板。要了解更多信息，请参见*创建 DHCP 强制实施器服务器*（第79页）。
   - **Maintenance Mode/Enforcer Override:** 当系统处于维护模式，或DHCP 强制实施器已通过 Override DHCP Enforcer 勾选框被禁用时，决定网络访问。
   - **Default:** 如果无法找到关联的访问模板时，决定网络访问。

6. 如果需要，使用箭头优先化访问模板。

   如果有多个模板应用到某个特定的状态中，第一个满足该状态的模板会被使用。Sophos建议您优先化较特别/严格的访问模板最先，较不特别/严格的访问模板次之。

7. 单击 **Save**。

2.5.4 创建 DHCP 强制实施器服务器

DHCP 强制实施器服务器用于强制实施 Sophos NAC DHCP 应用实施。要了解更多有关配置 DHCP 强制实施的信息，请参见 *Sophos NAC DHCP* 配置指南。

过程

1. 单击 **Configure System** > **Server Settings** 。单击页面左下方 **Create Server**。
2. 输入服务器的名称和描述。
3. 单击 **Server Type** 列表，然后选择 **DHCP Enforcer Server**。
4. 输入服务器的主机名或 IP 地址，然后，单击 **Add**。如果您输入主机名，NAC Manager 会试图解析该主机名为正确的 IP 地址。如果这不可能，那么，您必须输入正确的 IP 地址。
5. 输入和确认服务器的共享密钥 (shared key)。

   重要: 该共享密钥必须匹配，您在该服务器上安装 DHCP 强制实施器时，输入的共享密钥。

6. 选择未知终结点计算机模式，以指定DHCP强制实施器服务器是应该报告，还是应该强制实施未知的终结点计算机访问。

   Report Only 选项使您能够在不影响网络访问的情况下，展开部署 DHCP 强制实施器服务器。一旦您创建了 DHCP 免除项目，并且您的来宾用户使用 Dissolvable Agent，您就可以更改未知终结点计算机模式为 **Enforce**，以开启 DHCP 强制实施。

   未知的终结点计算机，没有受到 Sophos Enterprise Console的管理，没有被免除，并且要么没有运行 Dissolvable Agent，要么超越了 Dissolvable Agent 的遵照级别。

   注: 在未知终结点计算机模式中，在 **Configure System** > **Enforcer Settings** 区域中指定的 Unknown Endpoint 访问模板将决定网络访问。要了解更多信息，请参见 指定强制实施器设置（第76页）。

7. 单击 **Save**。

2.5.5 创建 Dissolvable Agent 服务器

Dissolvable Agent 服务器用户器用于托管 Dissolvable Agent。一旦定义之后，DHCP 强制实施器就可以允许访问这些服务器。

注: 如果您将 Dissolvable Agent 安装在 Sophos NAC 所在的同一个服务器上，那么，您不必创建额外的 Dissolvable Agent 服务器。

过程

1. 单击 **Configure System** > **Server Settings** 。单击页面左下方 **Create Server**。
2. 输入服务器的名称和描述。
3. 单击 **Server Type** 列表，然后选择 **Dissolvable Agent Server**。
4. 输入服务器的主机名或IP地址，然后，单击**Add**。如果您输入主机名，NAC Manager 会试图解析该主机名为正确的 IP 地址。如果这不可能，那么，您必须输入正确的 IP 地址。
5. 单击 **Save**。

2.5.6 更新 NAC 代理服务器设置

在安装 NAC 的过程中，您可以配置 NAC 使用代理服务器访问因特网。要求能够访问因特网，以便为安全应用程序下载最新的检测信息。使用此区域更新代理服务器设置，以及选择更新NAC Server IP 地址。

过程

1. 单击 **Configure System** > **Server Settings** 。
2. 单击 NAC Server 的名称，以更新它的服务器设置。
3. 或者，输入服务器的主机名或 IP 地址，然后，单击 **Add**。如果您输入主机名，NAC Manager 会试图解析该主机名为正确的 IP 地址。如果这不可能，那么，您必须输入正确的 IP 地址。

   重要: 因为 IP 地址决定代理和 NAC Server之间的连接，请确保它们准确无误。如果它们不正确，代理将无法与 NAC Server 进行通讯。

4. 单击 **Proxy Settings** 列表，选择相应的代理服务器选项:
   - **No Proxy:** NAC Server 不使用代理服务器访问因特网。
   - **Use Proxy:** NAC Server 使用代理服务器访问因特网。代理服务器设置最初是在 NAC 的安装过程中定义的，可以在需要时进行更新。
   - **Use SEC Proxy Settings:** NAC Server 使用在 Sophos Enterprise Console 中定义的代理服务器设置访问因特网。只有 Sophos Enterprise Console 与 NAC 安装在同一台服务器上是，此选项才可用。如果选择了此选项，代理服务器设置必须在 Sophos Enterprise Console 中进行更新。

5. 更新代理服务器设置。

   注: 必须填写代理服务器的地址和端口。只有使用要验证身份的代理服务器时，才要求用户名，密码，以及确认密码。

6. 单击 **Save**。

2.5.7 更新下载帐户详情

NAC 使用下载帐户用户名和密码，为安全应用程序下载最新的检测信息。

过程

1. 单击 **Configure System** > **Download Account Details** 。
2. 更新用户名和/或密码。
   如果您是更新现有的密码，那么，您必须确认新密码。
3. 单击 **Save**。

3 NAC 工具

3.1 载入器工具

作为 Sophos NAC 的一部分来安装的载入器工具，可以使导入新的和更新后的应用程序和应用程序类型到它们的 NAC Databases。

3.1.1 导入应用程序

使用载入器工具，可以有两种方式导入应用程序。您可以使用应用程序定义 EXE 文件，调用载入器工具，并自动导入应用程序，或者，您可以通过 import.xml 文件使用命令行导入应用程序。Sophos 建议使用应用程序定义 EXE 文件，因为它会自动调用载入器，并且较使用命令行更容易导入应用程序和应用程序类型。Sophos 为所有公司提供应用程序定义 EXE 文件。

3.1.2 使用应用程序定义 EXE 文件导入应用程序

1. 从 Sophos 网站下载应用程序定义 EXE 文件。
2. 复制已下载的应用程序定义 EXE 文件到 Sophos NAC Server。
3. 双击 EXE 文件导入更新的应用程序和应用程序类型。

   注: EXE 文件会调用载入器工具，并自动安装更新的应用程序和应用程序类型。

3.1.3 使用 import.xml 文件手动导入应用程序

1. 从 Sophos 代表那里获得更新的 import.xml 文件。
2. 复制 import.xml 文件到 Sophos NAC Server。

3. 在命令行提示窗口中，要运行载入器工具以导入新的定义，请输入：
   C:\Program Files\Sophos\NAC\Loader\Loader.exe C:\import.xml。

   注：

   - 命令不区分大小写。命令行参数使用前斜杠 “/” ，然后参数名，可以选择跟随分号和参数值。例如：/ID:id。参数值可以包含后斜杠 “\” 和空格；不过，任何包含空格的 DOS 参数，都需要引号，例如："C:\temp\my key.xml".
   - 载入器工具假定您使用具有 SQL 访问权限的 Windows 帐户登录到 Windows。如果您没有使用具有 SQL 访问权限的帐户登录到 Windows，您可以使用以下 SQL 帐户运行载入器工具：Loader /L:SQL /ID:ID /PW:PW /F:import.xml（这里的 ID 和 PW 是有效的 SQL 帐户的 ID 和密码）。
   - 除了在以下章节中用下划线标出的 DOS 命令之外，您可以查看载入器工具中的其它选项，方法是键入：loader /?。
   - 依照默认值，任何显示的出错消息，同时会被记录到事件日志中。

3.1.4 导出应用程序

如果 Sophos 需要查看自定义的应用程序定义，您必须从命令行提示窗运行载入器，将数据导出到 Sophos。使用以下示例导出自定义的应用程序。

命令	描述
Loader /A:export /B:application /I:id /F:export.xml	通过唯一的 ID 导出某个应用程序。该应用程序的定义会被保存到指定的 XML 文件中。
Loader /A:export /B:application /N:"name" /F:export.xml	通过名称导出某个应用程序。该应用程序的定义会被保存到指定的 XML 文件中。
Loader /A:export /B:application /n:* /F:export.xml	导出所有的应用程序到指定的 XML 文件中。

3.1.5 载入器 DOS 命令

以下表格列出了载入器工具可以使用的 DOS 命令行。这些命令行可以用来将应用程序载入到数据库中，从数据库中导出应用程序，或者，在导入之前校验某个 import.xml 文件。要使用这些命令，请将它们作为命令行参数传递到载入器工具中。例如：表中的第一个命令，可以通过键入以下命令行，得到执行：
Loader /F:import.xml

命令	描述
/F:import.xml	从指定的 XML 文件中载入任何应用程序或应用程序类型。
/F:imp*.xml	从多个文件中载入应用程序或应用程序类型。
/B:application /N:"name" /F:export.xml	通过名称导出某个应用程序。该应用程序的定义会被保存到指定的 XML 文件中。

3.2 日志记录工具

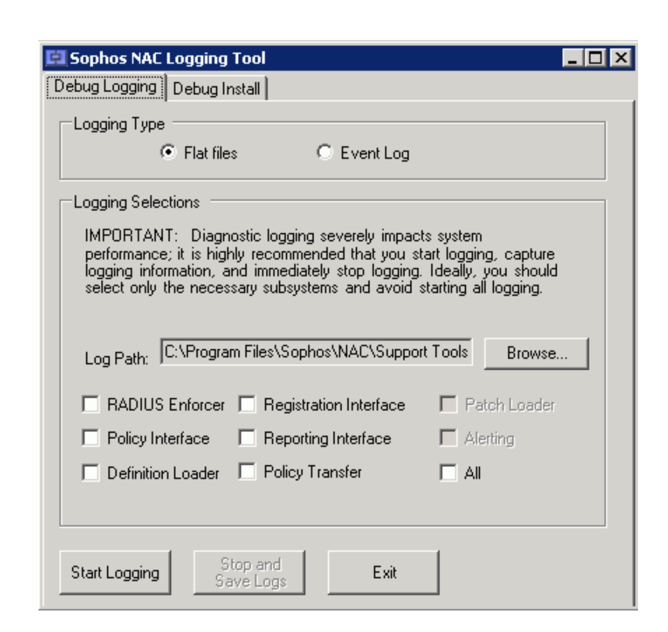
日志记录工具使您能够开启安装和子系统的日志记录，以便进行排疑解难活动。Debug Logging 标签页使您能够识别日志记录方法，文件路径，以及手动启动和停止所选择的子系统的日志记录。Debug Install 标签页使您能够识别要诊断的安装文件，以及日志记录文件的路径。日志记录设置为最高的级别；日志记录的信息，取决于执行的日志记录的类型。

重要: Sophos 建议您仅为排疑解难的目的而使用此工具，在 Sophos 的有关人员提出时，才这样做，并且您不要让日志文件总是处于启用状态，因为这样会给系统运行效率造成极大的影响。

3.2.1 Sophos NAC Server 子系统日志记录

1. 在 Sophos NAC Server 中找到日志记录工具。该工具所在的默认路径为: C:\Program Files\Sophos\NAC\Support Tools。

2. 双击 **LoggingUtil.exe**。



3. 在 **Debug Logging** 标签页中，选择相应的日志记录类型和日志记录选项，然后单击 **Start Logging**。

   要了解各个栏的有关信息，请参见*Debug Logging标签页的栏目及描述*（第85页）。

   注: 一旦您单击了 **Start Logging**，您就无法选择或取消选择附加的子系统。您必须停止日志记录，更改您的日志记录选项，并再次启动日志记录。

4. 在您想要获得日志记录信息的 Sophos NAC Server 上，执行相应的任务。
5. 一旦您执行了相应的任务，单击 **Stop and Save Logs** 以将日志记录信息保存到相应的日记记录文件中。

   文件将保存在您在 **Log Path** 栏中指定的路径。默认的日志路径是：C:\Program Files\Sophos\NAC\Support Tools\Logs。要了解日志文件类型以及它们包含的内容的有关信息，请参见日志文件（第88页）。

   注: 当日志记录为禁用时，**Stop and Save Logs** 按钮为灰白显示。

3.2.2 Debug Logging 标签页的栏目及描述

诊断性的日志记录文件会极大地影响系统运行效率。强烈建议您在启动日志记录，保存了日志信息之后，立即停止日志记录。最好是，您应该仅选择所需要的子系统，避免启动所有的日志记录。

注: 日志记录设置为最高的级别，包括日志记录出错消息，提醒消息，信息消息，完全追踪消息，以及调用堆栈消息等。

栏目	描述
日志记录类型	
Flat File	设置日志记录以生成平面文件(flat file)。会为您选择的每个子系统各创建一个平面文件。
Event Log	设置日志记录，添加子系统的信息到 Sophos NAC Server的事件日志(Event Log)。
日志记录选项	
Log Path	设置放置所生成的日志文件的路径。
RADIUS强制实施器	设置NAC Server的日志记录。此选项仅用于 DHCP 强制实施。 NAC Server，是为 DHCP 强制实施器检查代理遵照结果的软件组件。
Policy Interface	为策略接口服务设置日志记录。 策略接口是服务器端的组件，它为代理获取策略，并校验代理请求的有效性。
Definition Loader	设置定义载入器的日志记录。 定义载入器是服务器端的组件，它负责安全应用程序检测，签名版本检测，扫描引擎版本检测，最近扫描日期检测，实施保护检测，启用功能检测，以及自动调整措施等。
Registration Interface	为注册接口服务设置日志记录。 注册接口是服务器端的组件，它为代理提供注册服务。在代理每次为首次注册者或重新注册者进行注册时，Registration Interface 会进行用户身份验证。
Reporting Interface	为报告发送接口服务设置日志记录。 报告发送接口是服务器端的组件，它接受来自代理的报告发送数据。报告发送接口还校验代理请求的有效性。

栏目	描述
Policy Transfer	为策略传送服务设置日志记录。 策略传送是从策略数据存储向报告数据存储传送数据的服务器端组件，以便已更新的策略信息在报告中得到体现。
All	为所有的 NAC 子系统设置日志记录。

3.2.3 Sophos NAC Server 安装日志记录

此工具只应该被用于安装过程中的排疑解难。您应该首先安装 Sophos NAC。如果在初始安装过程中出现错误，您可以使用该工具获取有关安装的日志记录信息。

1. 在 Sophos NAC Server 中找到日志记录工具。该工具所在的默认路径为: C:\Program Files\Sophos\NAC\Support Tools。
2. 双击 **LoggingUtil.exe**。
3. 单击 **Debug Install** 标签。
4. 为您想要进行排疑解难的安装文件选择合适的路径，以及选择您想要放置日志文件的路径，然后，单击 **Start Install**。

   要了解各个栏的有关信息，请参见*Debug Install 标签页的栏目及描述*（第87页）。

   注: 一旦安装完成，文件会被保存到您在 **Log Path** 栏中指定的路径。默认的日志路径是: C:\Program Files\Sophos\NAC\Support Tools\Logs。要了解日志文件类型以及它们包含的内容的有关信息，请参见日志文件（第88页）。

3.2.4 Debug Install 标签页的栏目及描述

日志记录设置为由 Microsoft® Windows® Installer 决定的最高的级别。

栏目	描述
Install File Path	选择安装文件的路径。
Log Path	设置在安装过程中生成的日志文件放置的路径。

3.2.5 日志文件

默认的日志文件路径是：C:\Program Files\Sophos\NAC\Support Tools\Logs，该路径在 Sophos NAC Server上。在生成日志文件之前，可以更改该路径。每次日志记录启动后，任何在指定的路径中的同名文件都会被覆盖。

栏目	描述
AppEvent.xml	包含从 Sophos NAC Server上的 Event Log 中导出的应用程序事件的文件。当 Event Log 选项作为日志记录类型被选择时，子系统的日志信息包括在此文件中。
SystemEvent.xml	包含从 Sophos NAC Server上的 Event Log 中导出的系统事件的文件。Internet 验证服务 (IAS) 信息包括在此日志文件中。
Systeminfo.nfo	包含有关 Sophos NAC Server上的硬件和操作系统信息的文件。
UserInfo.txt	包含供用户用来登录 Sophos NAC Server 的帐户信息，例如帐户名称和权限，以及供已安装的子系统运行的帐户信息的文件。
<Subsystem>.xml	包含 Sophos NAC 子系统日志信息的文件。 当 Flat File 选项作为日志文件类型被选择时，NAC Server 子系统会分别保存到不同的平面文件(flat file)中，注释见下： ■ Policy Interface:PolicyInterfaceLog.xml ■ Definition Loader:CurrentDefsLoaderLog.xml ■ Registration Interface:RegistrationInterfaceLog.xml ■ Reporting Interface:ReportingInterfaceLog.xml ■ Policy Transfer:PolicyTransferLog.xml
Install<datetime>.log	Microsoft Windows Installer 输出文件包含有关安装的信息。 此文件仅作为 Debug Install 标签页的功能来生成。
SophosNACLogs.zip	包含所有 Debug Logging 标签日志文件的文件。
InstallLogs.zip	包含所有 Debug Install 标签日志文件的文件。

3.3 维护模式工具

当您执行数据库维护，和/或处理网络问题或数据库问题时，使用维护模式工具。此工具是命令行工具，用来开启或关闭维护模式。此工具会停止相应的 Sophos NAC 服务，以便您能够执行所要求的维护。一当您准备返回工作状态，请停止维护模式工具。此工具会自动启动被停止的服务。

当 Sophos NAC 处于维护模式时，Sophos Compliance Agent 会识别该模式，并在执行时不向发送出错消息，没有干扰，不告知用户处于维护模式中。代理将在本地保存所有的评估和报告信息，直到软件返回工作模式。同时，代理继续针对缓存中的策略进行评估，并且如果使用了代理隔离，终结点计算机仍然可以基于缓存中的策略的规则而被隔离。另外，如果您使用 DHCP 强制实施，DHCP 强制实施器访问模板，以及免除项目会被缓存，所有的 DHCP 请求，将被使用缓存的 DHCP 强制实施管理器访问模板和免除项目。

注: 在 NAC 升级时，您不需要使用此工具。NAC 的安装过程，会将 NAC Server 放入维护模式中，并在安装完成时，使服务器脱离维护模式。

3.3.1 运行维护模式工具

1. 从 Sophos NAC Server 上的命令行提示窗中，进入 C:\Program Files\Sophos\NAC\Support Tools 目录。
2. 键入 **MaintMode.exe /start**。该命令会将 Sophos NAC 置于维护模式。
3. 键入 **MaintMode.exe /stop**。该命令会将 Sophos NAC 返回工作模式。

3.3.2 维护模式工具命令

命令不区分大小写。命令参数使用前斜杠 “/” ，然后参数名。任何包含空格的 DOS 参数值都要求引号。

命令	描述
MaintMode.exe /start	启动维护模式工具。
MaintMode.exe /stop	停止维护模式工具。
MaintMode.exe /E:silent	指定没有消息写入命令行对话框。出错消息将总是被写入事件日志。
MaintMode.exe /E:error	指定只有出错消息将写入控制台。出错消息将总是被写入事件日志。

命令	描述
MaintMode.exe /E:warn	指定只有出错消息和提醒消息将写入控制台。出错消息将总是被写入事件日志。
MaintMode.exe /E:info	指定出错消息，提醒消息，以及信息消息将写入控制台。出错消息将总是被写入事件日志。
MaintMode.exe /?	显示维护模式工具帮助窗口。

4 用语表

这是 Sophos NAC 用语表。

访问状态　访问状态，是指某个可以应用来决定网络访问的访问模板的任何状态。代理强制实施器访问模板，可以应用于策略中的访问状态。DHCP 强制实施器访问模板，可以应用于策略，免除条件，以及强制实施器设置中的访问状态。

访问模板　访问模板，当它们与策略，免除项目，以及强制实施器设置（取决于强制实施类型）中的访问状态关联时，决定网络访问。

帐户　帐户由用户的登录名和安全角色组成。帐户名和密码被用来登录 NAC Manager。安全角色决定每个帐户的权限级别。

代理配置模板　代理配置模板，定义可选设置，以控制 Quarantine Agent 怎样在终结点计算机上工作。

代理强制实施器　代理强制实施器，是一种强制实施类型，它通过基于客户端的评估和隔离强制实施，保护运行 Quarantine Agent 的终结点计算机的网络。

代理会话进程　代理会话进程，是代理在终结点计算机上活动，并访问 Sophos NAC 的那段时间。

代理设置　代理设置决定代理在终结点计算机上运行时，代理的功能。您可以在创建代理配置时，指定代理设置。

所有策略行为　策略中某一类型的所有配置文件，都将在终结点计算机上进行评估，并且与所有配置文件相关的必要措施都会执行。所有行为使用终结点计算机上，**最低限度**遵照的配置文件来决定策略中的该配置文件类型的遵照状况。您想要在终结点计算机上避免的应用程序配置文件，也可以此方式被评估。

应用程序　应用程序是受 Sophos NAC 支持的软件应用程序。应用程序定义功能，关联条件，遵照状态，以及可能的措施。应用程序会与某个应用程序类型联系起来，以决定当该应用程序的配置文件被添加到策略中时，应该怎样评估该应用程序。

应用程序类型　应用程序类型，将应用程序分类，并为与应用程序类型关联的所有的应用程序建立默认的策略行为。

审核 审核是系统发生的事件的审核过程或历史记录。事件可以包括更新，新项目，或系统活动，如：更新到当前的策略，创建新的访问模板，或帐户登录/注销 NAC Manager。

最佳策略行为 策略中的某一特定类型的每个配置文件，都是在终结点计算机上被评估，最佳匹配的配置文件将被确定，并且只有与最佳匹配的文件有关的必要的措施会被执行。所有行为使用终结点计算机上，**最大限度**遵照的配置文件来决定策略中的该配置文件类型的遵照状况。应用程序配置文件，除非另有指定，都是以此方式被评估的。如果被评估的配置文件，没有任何一个安装到了终结点计算机上，那么，来自最优先的配置文件的“其它”的条件遵照状况，将被用来决定策略中的该配置文件类型的遵照状况和措施。

功能 能力是指某个应用程序的各种功能，这些功能可以作为遵照评估的一部分被检测。功能包括用于评估的规则，它由条件，遵照状态，信息，以及调整措施等构成。

遵照状态 遵照状态是通过对照配置文件中定义的条件，评估终结点计算机上的检测结果来决定的。然后，遵照状态会被映射到策略中相应的访问模板中，以决定实际允许的终结点计算机的网络访问。遵照状态可以为遵照，部分遵照，或未遵照。

条件 条件是指在评估时使用的陈述，它用于决定终结点计算机上的相关的遵照状态，以及将要采取的措施。

默认 如果没有找到关联的访问模板，那么，在 **Configure System** > **Enforcer Settings** 区域中定义的访问状态，将决定网络访问。

预设的默认策略 预设的默认策略是指用于，当某个终结点计算机已经安装了代理，并没有被指派其它策略时，所使用的策略。依照默认值，该策略模式设置为“仅限报告”模式。如果该策略模式设置为“调整”模式，或“强制实施”模式时，它可以执行调整措施。

检测规则 检测规则，指定将在终结点计算机上检测的，注册键值，进程，或文件，以便决定是否安装，运行，或需要特定版本或值的，某个应用程序。

DHCP 配置向导 DHCP 配置向导可以帮助您识别 Sophos NAC DHCP 应用实施一道使用的代理，调整，Dissolvable Agent，以及 DHCP 强制实施器服务器。

DHCP 强制实施器 DHCP 强制实施器，是针对 Sophos NAC DHCP 应用实施，为网络提供保护的强制实施类型。

Dissolvable Agent Dissolvable Agent 评估终结点计算机，以在允许网络访问之前，确定它们是否遵照 NAC 策略。Dissolvable Agent 必须从浏览器中运行。Dissolvable Agent 是为没有或不能在终结点计算机上安装代理，但仍然必须访问特定的网络资源的用户，如：合同商或来宾，而设计的。Dissolvable Agent 与 DHCP 强制实施一道使用。

终结点计算机 终结点计算机，是指试图连接到网络中的计算机。终结点计算机可以运行代理，例外，无代理，或未知。

强制实施策略模式 强制实施策略模式，指定指定终结点计算机对照策略中配置文件来被评估，报告信息在 NAC Manager 中生成。通过使用针对相应的访问状态的访问模板，会显示消息，会执行调整措施，会采取强制实施措施。

强制实施器设置 强制实施器设置，指定 DHCP 强制实施器，以及代理强制实施器的强制实施类型的强制实施详情。

免除 免除，指定当连接到网络中时，不需要评估遵照的终结点计算机。免除项目，包括不能运行代理的终结点计算机，如：运行非 Windows 操作系统的终结点计算机；或者，包括不要求进行遵照评估的终结点设备，如：服务器，路由器，打印机。另外，为了在整个企业中分阶段进行阶段性强制实施，您可以为此免除任何您不想要被强制实施的终结点计算机。

维护模式/强制实施器覆盖 当系统处于维护模式或 DHCP 强制实施器被禁用时，在 **Configure System** > **Enforcer Settings** 区域中定义的访问状态，将决定网络访问。

受管理的终结点计算机 受管理的终结点计算机是指受到 Sophos Enterprise Console 管理，并安装了 Sophos Compliance Agent 的终结点计算机。受管理的终结点计算机使用 Quarantine Agent 进行遵照评估，以及获得网络访问。

受管理的策略 预设的受管理的策略可以用于，受 Sophos Enterprise Console 管理的，安装了代理的终结点计算机。依照默认值，该策略模式设置为“仅限报告”模式。如果该策略模式设置为“调整”模式，或“强制实施”模式时，它可以执行调整措施。

消息 在遵照评估期间，显示在终结点计算机上的信息消息或出错消息。只有当与之相关联的条件被满足时，消息才会在终结点计算机上显示。消息可用于所有的功能。

网络资源 网络资源是进行终结点计算机调整所要求的应用程序或设备，或者，终结点计算机应该被拒绝访问的应用程序或设备。网络资源，既可以添加到代理强制实施器的访问模板中，也可以添加到 DHCP 强制实施器的访问模板中。

无代理托盘 如果代理没有在终结点计算机上运行，那么，在策略中定义的访问状态将决定网络访问。此状态会由代理强制实施器报告，如果用户没有登录到Windows或者，代理托盘应用程序不再运行。

策略 策略，根据终结点计算机上的配置文件评估，控制访问企业网络资源。策略，管理决定终结点遵照状态，消息显示，执行的调整措施，采取的强制实施措施的配置。

策略行为 策略行为决定怎样，比照终结点计算机上的相同类型的其它配置文件，来评估配置文件。选项包括要求，最佳，以及所有。要了解更多的信息，请参见要求的策略行为，最佳策略行为，以及所有策略行为的定义。

策略获取错误（代理） 当无法为终结点计算机获取策略时，策略中定义的访问状态决定网络访问。如果代理无法从 Sophos NAC 服务器获取策略；或者，根据 **Configure System** > **Enforcer Settings** 区域中配置的代理策略更新级别，终结点计算机遵照状态尚未更新，那么，便会存在此状态。

策略获取错误 (DHCP) 如果根据在 **Configure System** > **Enforcer Settings** 区域中配置的 DHCP 策略更新级别，终结点计算机遵照状态尚未更新，那么，在策略中定义的访问状态将决定网络访问。

配置文件 配置文件允许您定义您想要在终结点计算机上评估的项目，如：操作系统，以及应用程序。配置文件定义条件，遵照状态，消息，以及调整措施。一旦创建了配置文件，它可以在策略中被组织，以及优先化。

配置文件类型 配置文件类型分类配置文件。配置文件会被放置到策略中，并根据类型和与之关联的策略行为，在终结点计算机上相互对比评估。

Quarantine Agent Quarantine Agent 评估终结点计算机，以确定它们是否遵照 NAC 策略。评估在网络访问被允许之前进行，被在网络访问

被允许之后，定期进行。代理要求很少或不要求用户的介入。Quarantine Agent 具有隔离功能，它提供强制实施，并在终结点计算机没有遵照 NAC 策略时，将它们限制在网络中的指定区域。

调整策略模式	调整策略模式，指定指定终结点计算机对照策略中配置文件来被评估，报告信息在NACManager中生成。会显示消息，会执行调整措施；不过，不会采取强制实施措施。
调整措施	在遵照评估期间，在终结点计算机上执行的措施，以使终结点计算机遵照策略。调整措施不能用于所有的应用程序或应用程序功能。
仅限报告策略模式	仅限报告模式，指定指定终结点计算机对照策略中配置文件来被评估，报告信息在 NAC Manager 中生成。不会显示消息，不会执行调整措施，以及不会采取强制实施措施。
要求的策略行为	操作系统的配置文件是必需的，并且将作为首选的配置文件进行评估。如果所需的操作系统之一没有安装到终结点计算机上，那么，来自最优先的操作系统的配置文件的“其它“的条件遵照状况，将被用来为该未安装的操作系统配置文件类型决定遵照状况和措施，并且不会评估该策略的任何附加的配置文件。
安全角色	安全角色，决定各NACManager帐户的权限级别，它在创建帐户时被指派。
未知的终结点计算机	当没有遵照记录存在时，在 **Configure System** > **Enforcer Settings** 区域中定义的访问状态，将决定网络访问。未知的终结点计算机，没有受到 Sophos Enterprise Console的管理，没有被免除，并且要么没有运行 Dissolvable Agent，要么超越了 Dissolvable Agent 的遵照级别。当 DHCP 服务器处于 Report Only 或 Enforce 未知终结点计算机模式时，您可以选择针对未知的终结点计算机使用的访问模板。、
未受管理的终结点计算机	未受管理的终结点计算机是指没有受到 Sophos Enterprise Console 管理，来自公司外部的终结点计算机。未受管理的终结点计算机使用 Dissolvable Agent 进行遵照评估，以及获得网络访问。
未受管理的策略	预设的 Unmanaged 策略，用于来自公司外部的终结点计算机。此策略**不会**在终结点上执行调整措施。Dissolvable Agent 使用未受管理的策略。

用户覆盖	如果用户覆盖了在终结点计算机上隔离的代理，那么，在策略中定义的访问状态将决定网络访问。如果用户覆盖了隔离状态，隔离状态会被禁用。

5 技术支持

使用 文档，搜索与您的疑问，问题，或故障相关的信息。

如果您无法找到答案，请访问 *http://www.sophos.com/support*。如果您要联系技术支持，请尽量准备好以下信息:

- Sophos 软件的版本号。
- 操作系统及其补丁包级别，如果有。
- 任何出错信息的原文。

6 版权所有

索引

字母

A

B

C

D

F

G

J

K

L

M

P

Q

R

S

T

W

X

Y

Z